12-24-2015

Investigation of Electromagnetic Signatures of a FPGA Using an APREL EM-ISIGHT System

Karynn A. Sutherlin

INVESTIGATION OF ELECTROMAGNETIC SIGNATURES OF A FPGA USING AN APREL EM-ISIGHT SYSTEM

THESIS

Karynn A. Sutherlin, Civilian, DAF

AFIT-ENV-MS-15-D-035

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENV-MS-15-D-035

INVESTIGATION OF ELECTROMAGNETIC SIGNATURES OF A FPGA USING AN APREL EM-ISIGHT SYSTEM

THESIS

Presented to the Faculty

Department of Systems Engineering and Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Systems Engineering

Karynn A. Sutherlin

Civilian, DAF

December 2015

AFIT-ENV-MS-15-D-035

INVESTIGATION OF ELECTROMAGNETIC SIGNATURES OF A FPGA USING AN APREL EM-ISIGHT SYSTEM

Karynn A. Sutherlin, Civilian, DAF

Committee Membership:

Lt Col K. F. Oyama, PhD
Chair

Dr. M. R. Grimaila
Member

Mr. G. D. Via
Member

Abstract

Large military platforms have encountered major performance and reliability issues due to an increased number of incidents with counterfeit electronic parts. This has drawn the attention of Department of Defense (DOD) leadership making detection and avoidance of counterfeit electronic parts a top issue for national defense. More defined regulations and processes for identifying, reporting, and disposing of counterfeit electronic parts are being revised to raise awareness for this issue, as well as enhance the detection of these parts. Multiple technologies are currently employed throughout the supply chain to detect counterfeit electronic parts. These methods are often costly, time-consuming, and destructive. This research investigates a non-destructive test method that collects radiated electromagnetic emissions from functional devices using a commercially available system, the APREL EM-ISight. A design of experiments (DOE) is created and executed to determine the significant system factors and interactions. These factors are then optimized for the desired responses. The sensitivity of the system is analyzed by scanning a commercial-off-the-shelf (COTS) field-programmable gate array (FPGA) at the optimized factor levels established from the DOE and varying the programmed signal. This research established the viability of using APREL's EM-ISight to detect a device's inherent electromagnetic signature by successfully identifying a defective board and characterizing the process variations of multiple boards. Another conclusion of this research is the tradeoff between resolution and scan time.

Acknowledgments

There are many people I would like to acknowledge for their support throughout this endeavor. I would like to express my sincere appreciation to my committee: Lt Col Oyama, Dr. Grimaila, and Mr. Via, for their guidance and support throughout the course of this thesis effort. The insight and experience you provided was certainly appreciated. There are many colleagues and friends that contributed their time, troubleshooting skills, and good ju ju towards this research. They include Mr. Ryan Gilbert, Mr. Wil Gouty, Mr. Marc Hoffman, Mr. Steve Tetlak, and Mr. Jim Alverson. I greatly appreciate your effort, encouragement, and a good laugh here and there during these past few months. Thank you. Finally, I would like to thank my family for their love, positive attitude, and their simplistic view on making everything sound so much easier than it really is and for encouraging me that the light at the end of the tunnel is not a train but the happy sun.

Karynn A. Sutherlin

Table of Contents

List of Figures

Page

List of Tables

Page

List of Equations

INVESTIGATION OF ELECTROMAGNETIC SIGNATURES OF A FPGA USING AN APREL EM-ISIGHT SYSTEM

I. Introduction

General Issue

Over the last 15 years, an increasing number of counterfeit electronic parts have become a critical issue for both industry and the Department of Defense (DOD) (Aerospace Industries Association, 2011). Everything from discrete electronic components and integrated circuits (ICs) to circuit boards are at risk. Based on the *Defense Industrial Base Assessment: Counterfeit Electronics*, a counterfeit part is not genuine if any of the following five criteria are met (U.S. Department of Commerce, 2010). It:

1. is an unauthorized copy
2. does not conform to original OCM* design, model, and/or performance standards
3. is not produced by the OCM or is produced by unauthorized contractors
4. is an off-specification, defective, or used OCM product sold as "new" or working
5. has incorrect or false markings and/or documentation

*OCM refers to the Original Component Manufacturer.

The total value of counterfeit electronic parts in the G20 economy was forecasted to cost between $1.2 and $1.7 trillion in 2015 (International Chamber of Commerce, 2011). In addition to the projected costs, security, safety, and reliability topics are other prime concerns associated with counterfeit electronic parts. The cost value of recycled and remarked parts is estimated to contribute to over 80% of all counterfeit parts in circulation (Kessler & Sharpe, 2010). U.S. companies were found to be largely unaware of any legal requirements or liabilities for the disposal of parts (U.S. Department of

Commerce, 2010). This ignorance in the US permitted electronic waste to be shipped to China for disposal. These shipments created a new market for organized crime and entrepreneurialship through disassembly and overhauling of components. Hence, China is the leading source for counterfeit components. These devices often make their way back into the hands of the consumer unnoticed. This research focuses on the detection of reused counterfeit parts using a proposed new method of scanning to detect a variation in the 3-D electromagnetic signature at the board level.

Problem Statement

Counterfeit electronic parts are infiltrating major program systems resulting in compromised integrity that degrades system reliability and performance. It is desirable to be able to test electronic parts to identify counterfeit electronic parts in a nondestructive, cost and time efficient manner with a high level of confidence. Analyzing a part's unique electromagnetic signature using APREL's EM-ISight automated system is hypothesized to be a novel way to accomplish this task.

Research Questions

The research questions below addresses the overall focus of this thesis.

- What are counterfeit electronic parts?
- How can counterfeit electronic parts be detected?
- How can reused electronic parts be detected?

Investigative Questions

The following investigative questions support the study of the research question.

- Can counterfeit electronic parts be detected using the part's unintentional electromagnetic signature?
- How effective is the APREL EM-ISight at detecting counterfeit electronic parts?
- What is the optimal test setup to detect counterfeit electronic parts?
- How repeatable are the test results?

Research Focus

The scope of this research focuses primarily on item four in the general issue discussion above, "an off-specification, defective, or used OCM product sold as "new" or working" (U.S. Department of Commerce, 2010). A commercial-off-the-shelf (COTS) board containing a field programmable gate array (FPGA) is the circuit board utilized for testing the inherent electromagnetic signature. Every device produces an internal electromagnetic emission (EME). Often, these emissions interfere with other parts on the board and a unique electromagnetic signature is created. The FPGA can be reprogrammed to allow for a potential new electromagnetic signature based on component functionality. These signatures are collected and analyzed using the APREL EM-ISight system.

Methodology Overview

The methodology implemented for this research is a three step process. The first step researches current counterfeit parts detection techniques in Chapter II. The second phase is composed of conducting several tests. In this phase a design of experiments (DOE) is implemented to optimize the test routine. Then, a comparative study is

conducted between several COTS boards to determine manufacturing process variations. A sensitivity analysis is also accomplished to determine the system boundaries for identifying minor deviations. The third and final stage is a comprehensive analysis of all the data collected to determine the effectiveness of an electromagnetic signature in determining a counterfeit part.

Assumptions/Limitations

The most significant assumption in this research is that the circuit boards examined in this thesis are "known good" parts and are indeed not a counterfeit. Having an untampered new part is imperative to the baseline results. The only verification of this assumption was optical examination and inspection of the parts and documentation upon arrival. One limitation of the unit of analysis, in this research, is the chip and not individual components. With the emphasis placed at the chip level, a variation in the electromagnetic signature can occur due to one or more components or a combination of components being reused, damaged, or failing.

Another limitation potentially involves the capability of the equipment used to detect counterfeit parts. An electric field (E-field) is the amount of electric force per unit charge. Electric fields can be created by the change in magnetic fields. A magnetic field (H-field) is the force on moving a charge. Magnetic fields are produced by the flow of electrons that create a current. Both fields show the behavior of an operational device and exhibit how signals and waves propagate inside the device. The EM-ISight tool is limited to a 0.03 mm spatial resolution for the E and H-field probes. The frequency range is also limited based on the probe, low noise amplifier (LNA), and spectrum analyzer. The probe

selected in this research has a maximum frequency range of 6 GHz. In this case, the study will only use a frequency range of 50 MHz to 550 MHz.

Implications

The ability to detect reused counterfeit parts sold as new will be useful for both industry and DOD. The National Defense Industrial Association (NDIA) defined the procurement process, and more specifically the detection and avoidance of used counterfeit parts, as one of their top issues in 2014 (National Defense Industrial Association, 2014). The financial liability for the repair or replacement of counterfeit electronic parts is a major concern since the parts are usually introduced several levels deep in the supply chain. These liabilities can often bankrupt small businesses. This test procedure could be an effective way to determine the authenticity of devices currently implemented in major programs without destroying the unit. In addition, it could be a way to determine the health status of the system after use in stressful test conditions. This can aid in the lifetime maintenance and functionality of the overall system.

Preview

The remainder of this research is divided into four additional chapters. Chapter II provides a literature review of current counterfeit detection techniques and recent tests on electromagnetic emission and signature variations and their causes. Chapter III delivers a detailed methodology of the research and test protocol. Chapter IV discusses the analysis and results drawn from the data collection. Chapter V concludes the thesis with recommendations acquired from this research and new opportunities for future research.

II. Literature Review

Chapter Overview

Chapter II focuses on several topics of interest for this research including (1) the effect of counterfeit parts on the government, industry, and consumers; (2) current methods for detecting counterfeit parts; (3) preventative measures to deter counterfeiting; (4) recent research on electromagnetic emissions and signatures; and (5) a brief overview of the APREL EM-ISight tool. The first topic discusses major concerns and vital statistics regarding counterfeit items that plague the electronics world. The second subject discusses, in more detail, the approaches currently used to identify counterfeit parts. The third item examines some of the procedures, policies, and new device technology that are being implemented to make new parts less susceptible to counterfeiting and to prevent the purchasing of counterfeit items. The fourth topic investigates research topics and current results from electromagnetic emission/signature tests. Finally, an overview of the system utilized in this research will be described.

Statistics and Impacts from Counterfeit Parts

The government has tracked and reported the increase of electronic counterfeit parts over the past 15 years. The Bureau of Industry and Security (BIS) assessment focused on five segments of the supply chain – the Original Component Manufacturer (OCM), distributors and brokers, circuit board assemblers, prime contractors/subcontractors, and DOD agencies; that investigated 387 companies and organizations over a three year period between 2005 to 2008 (U.S. Department of Commerce, 2010). Over this time period, the BIS documented the annual number of

counterfeit electronic incidents across the industry rose from 3,868 to 9,356. Out of the 387 companies and organizations investigated, 39% encountered counterfeits at least once during this time period. The majority of these incidents occurred at the OCM level of the supply chain and were typically found in microcircuits, as opposed to discrete devices like capacitors, resistors, and inductors. A notable concern is the increase in the number of incidents on the Qualified Products List (QPL) and Qualified Manufacturers List (QML). Over three years, the number of incidents increased tenfold. This is a concern since many DOD entities purchase items from this approved list and about 60% of the authorized distributors had an incident with counterfeit electronics (U.S. Department of Commerce, 2010).

From a 2009 survery, conducted by the US. Department of Commerce, 55% of distributors used internal, contractor, or both types of testing facilities to detect counterfeit parts. In the other segments of the supply chain less than 55% of companies conduct testing for counterfeit products, with only 11% of board assemblers completing testing. Used products, marked as new or higher grade, account for the majority of incidents found during the survey. The survey also found most of these products came from China at every level of the supply chain.

Counterfeit electronic parts are making their way through the supply chain and into consumers' hands. Starting with the Organisation for Economic Co-operation and Development's (OECD) original estimates from their 2005 data, the International Chamber of Commerce (ICC) launched a business initiative in 2011 called the Business Action to Stop Counterfeiting and Piracy (BASCAP) to estimate the global econmic and social impacts caused by counterfeiting and piracy. They estimated in 2015 the total

value of counterfeit and pirated products for the G20 economies will be between $1.2 and $1.7 trillion dollars. Furthermore, 2.5 million jobs have already been lost due to counterfeiting and piracy (International Chamber of Commerce, 2011).

There are various impacts to government, industry, and consumers from the introduction of counterfeit products. National security and safety are the primary concerns for the U.S. Government, in addition to loss of tax revenues. Counterfiet electronic parts found in companies cause damage to their business image and ultimately lead to a loss of sales and an imposed cost to replace failed parts and mitigate the risk of future encounters. After customers insert counterfeit items into their intended system, associated costs due to failure, lower quality, or poor reliability can escalate the maintenance and/or replacement cost. Degraded performance is a leading concern to the end user (Rostami, Koushanfar, & Karri, 2014). When faulty parts are placed in major vehicles, such as a satellite, a whole program/mission can be terminated when a single part fails. Additionally, safety is always a prime concern, especially on manned platforms. Counterfeit electronic parts pose a threat to every person, company, and platform that interacts with the item (Aerospace Industries Association, 2011).

Detection Methods

Current counterfeit parts can be categorized into two major types of defects: (1) physical defects and (2) electrical defects (Guin, DiMase, & Tehranipoor, 2014). Physical defects can be detected by optically inspecting the exterior of the part for labeling inconsistencies, damaged leads or bonds, dimension analysis, blacktop testing, etc. Interior tests such as material analysis, X-Ray scans, de-lidding, Scanning Acoustic

Microscopy (SAM), Scanning Electron Microscopy (SEM), and Raman Spectroscopy are examples of the standard practices to find physical defects in counterfeit parts. Electrical defects are more difficult to detect and often require extensive characterization to determine if the item is a counterfeit. Group A testing is comprised of a "device's full functional and parametric requirements at the recommended manufacturer's or specific industry extreme operating temperatures" (Frederico, 2009). In addition to Group A testing, burn-in tests and accelerated life testing is utilized to predict device performance. Taxonomies of counterfeit component types, the detection methods, and defects/anomalies found in counterfeit electronic components are included in Appendix A (Guin, DiMase, & Tehranipoor, 2014).

A major focus is being placed on stricter standards, trusted supply chain assurance, certification testing, secure/anti-tamper chips, and new device identification methods. However, this research concentrates on investigating a robust technique for detecting counterfeit parts, especially for identifying functional, reused parts that are most likely labeled at a higher quality than the manufacturer originally intended. It uses a non-destructive and cost effective method to collect and compare parts' radiated emissions to identify major changes in the parts tested.

Before Buying Parts

Before buying parts, several tasks can be completed to ensure the purchase is from a reliable source. If possible, replacement parts should be purchased from the OCM or Original Equipment Manufacturer (OEM). Simple tactics such as reviewing "product documentation, shippers, etc. in excruciating detail" prior to acquisition can help safeguard against buying counterfeit parts (Lowry, 2007). Watching for misspellings,

grammar issues, abnormal expressions, and wrong information when compared to original product documentation can be indications of a counterfeit supplier. Another warning sign when looking up items online are short-lived websites. This is a good indicator that the supplier is illegitimate. A way to confirm this suspicion is to utilize either an internal or public Qualified Suppliers List for Distributors (QSLD) or a Qualified Suppliers List for Manufacturers (QSLM) (Aerospace Industries Association, 2011).

External Visual Inspection and Testing

Upon receipt, regardless of the supply chain level, external visual inspection is typically the quickest and least expensive method to detect simple counterfeiting techniques. For example, basic inconsistencies in logo, part number, documentation (or lack thereof), shipping material, spelling errors, and legibility are obvious clues the part has been tampered with and is most likely a counterfeit. If the part passes a rudimentary optical inspection a more detailed investigation can be completed. Physical defects such as dimensions, corrosion, color, lead straightness, and electrostatic discharge (ESD) damage may indicate improper handling or reuse of parts (Lowry, 2007; Guin et al., 2014; Frederico, 2009).

A more thorough investigation of the part includes checking for signs of sanding, blacktopping, and marking permancy. Blacktopping can consist of sanding packaged devices down and then applying an epoxy with the shavings to create a new coating on the package. It is then typically painted black (the color of the package) and then printing a new logo to the exterior. One indicator of a counterfeit part is if the logo is smudged, coming off, or partially gone. Using certain slovents can often times remove labels or the

blacktopping to show the original package. Figure 1 shows two characteristics of counterfeit parts.

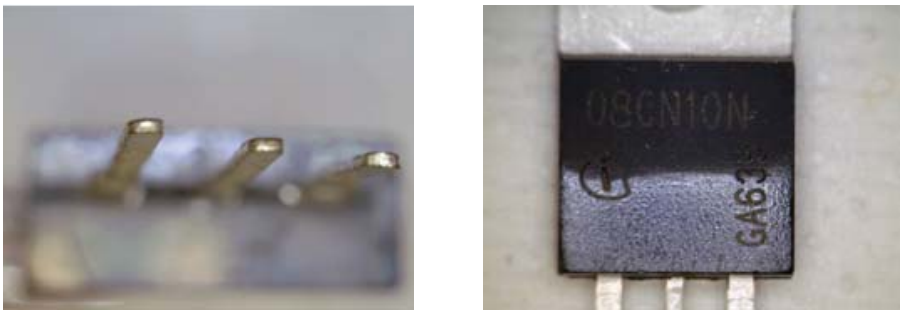


Figure 1 Example of lead tampering (left) and blacktopping (right). (In Compliance, 2010)

Non-Destructive Imaging and Testing

Inspecting a part without destroying it is preferred when selecting a detection method for the sake of reporting the part, getting a second opinion, or actually using the component if it is a non-counterfeit part. In addition to testing, there are a number of non-destructive imaging techniques used to inspect the wire bonding of the pins and conduct a material analysis. A common practice is X-ray analysis which allows the user to look through the component's package to inspect the internal structure of the part including the workmanship, location, and size or wire bonds (Lowry, 2007; Guin et al., 2014; Frederico, 2009).

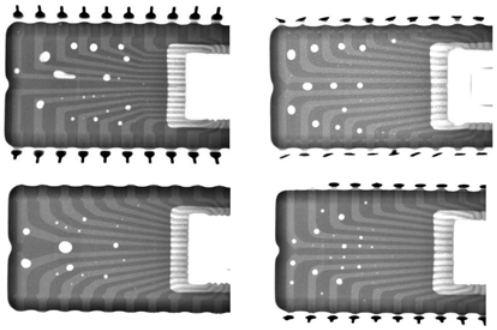


Figure 2 X-Ray images of four identically marked components showing different internal structures. (In Compliance, 2010)

A number of costly, yet effective, microscopy scans can be conducted to determine the authenticity of an electronic part. These techniques include scanning acoustic microscopy (SAM), scanning electron microscopy (SEM), energy-dispersive X-ray spectroscopy (EDXRS), Fourier transform infrared spectroscopy (FTIR), energy-dispersive X-ray fluorescence (EDXRF), and Raman spectroscopy. Although many of these techniques are non-destructive, they can include some sample preparation in order to characterize the device effectively. Some of the preparations include de-lidding, de-capping, thinning, or coating samples. SAM refers to a technology that transmits an ultrasound wave through a medium and the reflected signal can be detected, processed, and developed into an image (Delta, 2015). In SEM analysis, a focused beam of high-energy electrons produces a variety of signals from a sample. The interaction from this beam can create an image of the topography, "the external morphology, chemical composition, crystalline structure, and orientation of materials that make up the sample" (Frederico, 2009). EDXRS uses X-ray excitation interaction with the sample to determine the chemical characterization or elemental analysis of a sample. FTIR uses a Fouirer transform to convert raw data into a spectrum in order to identify organic or inorganic chemicals that elude to the type of polymer, coating, or contaminant on the device (Frederico, 2009). EDXRF is similar to EDXRS except that a detector is used to convert X-ray energy into voltage signals and then processed and analyzed into data to be able to characaterize individual particles. Raman spectroscopy uses the scattering of light to observe vibrational modulation which ultimately characterizes material and crystallographic orientation of a sample. All of these techniques are beneficial and used

under certain circumstances. Table 11 in Appendix A depicts which test methods detect certain types of defects identifed in the different types of counterfeit electronic parts.

Destructive Imaging and Testing

When non-destructive testing is inconclusive, destructive procedures can be employed. An easy test to conduct is a hermiticity test on packaged parts. This test checks a supposedly sealed package for any leaks (Guin et al., 2014; Lowry, 2007). De-capsulation/de-lidding allows the internal design to be inspected and check for any flaws or unprofessional workmanship in the bonding process. Focused ion beam (FIB) images often consist of some type of etch and/or deposition of material from/to the sample in order to obtain an appropriate image.

Electrical testing is one of the best ways to verify if a part is either good or faulty. Basic functional and parametric tests should be conducted based on the manufacturer's operational conditions (Lowry, 2007; Guin et al., 2014; Frederico, 2009). An initial burn-in test ensures the reliability of the device. Operating the part at an elevated temperature induces a ceratin amount of stress on that part. This test can easily detect defective or lower grade parts (Guin et al., 2014). Accelerated life testing (ALT) is a time consuming endevor for quality parts. Month-long tests are run to determine functional performance and operational conditions. It stresses the device at high voltage(s) and temperature(s). This testing rapidly ages and degrades the device. Early failures can be characaterized into specific failure modes as shown in Figure 35 of Appendix A.

Avoidance Methods

Today, emphasis is being placed on exhaustive processes, trusted supply chain assurance, certification testing, new device identification, and anti-tamper designs. Raising awareness and new technological designs are imperative to ensure the security and integrity of quality parts, as well as decrease the number of counterfeit items reproduced or repurposed. Whether a company is purchasing or fabricating products, there is a secure process to follow to help ensure the reliability of those components. Both of these topics will be discussed in more detail.

Awareness and Process Countermeasures

Increased awareness on the part of manufacturers, government agencies, and consumers is vital to reducing the number of counterfeit parts in everyday products and major programs (U.S. Department of Commerce, 2010). The Aerospace Industires Association (AIA) special report on counterfeit parts suggests a number of options that could be adopted or implemted to bring attention to this issue and some practices to ensure quality parts. The report includes topics such as "procurement, reporting, disposition, obsolescence and electronic waste" (Aerospace Industries Association, 2011). Adopting a standard such as AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition allows for uniformity across the industry and helps mitigate the risk of purchasing and installing counterfeit items. If a standard process is not implemented, developing and/or instating an internal purchasing process would help reduce risk as well. This process should include a review of approved manufactures/suppliers through a QSLD/QSLM and reports of suspected counterfeit parts through a database such as Government-Industry Data Exchange Program (GIDEP).

Training employees is an important factor in fortifying a compnay's ability to identify couterfeit parts. Applying an inspection checklist encompassing visual checks, electrical tests, investigative imagery, and other procedures upon arrival of new items will allow supply chains and consumers to increase the liklihood of finding a counterfeit part prior to installation. Documenting these procedures, in addition to a list of screened/approved suppliers, component pedigrees, and lifcycle analysis tools in a control plan is a good practice for companies to prepare. This allows the company to evaluate component obsolescence when making major design decisions. During this process, if a counterfeit part is found, it is essential to report this issue with an unbiased reporting organization such as GIDEP. Not only do they document the item, but they allow the manufacturer to investigate the claim. The AIA report stresses that the company does not return the suspicious part to the vendor. If it is a counterfeit it will just get recirculated. Therefore, in this case it is recommended that the part be destroyed. (Aerospace Industries Association, 2011).

Technical Countermeasures

Technology is quickly evolving to ensure the security of electronic devices to compete against the growing counterfeit trade. Unique identifiers can be integrated at the chip or package level. At the chip level, Physically Unclonable Functions (PUFs) use unique intrinsic features from a circuit as identification. PUFs exploit basic process variations, both physical and environmental, that exist in ICs which are unpredictable and uncontrollable (Wang and Tehranipoor, 2010). These unique features are easy to create but almost impossible to duplicate, making them ideal for anti-tamper applications. These embedded signatures are all stored in a vendor's secure database for future comparison.

Intellectual property (IP) rights are playing a major role in keeping ICs secure and protected. Techniques like hardware metering and Secure Split Test (SST) rely on IP rights. Hardware metering makes a small part of the design programmable at the time of configuration and then must be configured at the manufacturer. This process creates a unique chip ID that is difficult to reverse engineer (Koushanfar and Qu, 2001). Active metering locks every device until it is unlocked by the IP holder. Similar to hardware metering, "SST reestablishes trust into the IC fabrication and test process by reintroducing the IP owner in the IC testing procedure without requiring them to be physically present at the foundry/assembly" (Contreras, Rahman and Tehranipoor, 2013). Both procedures help prevent different types of counterfeit items.

The Defense Advanced Research Projects Agency (DARPA) has initiated several programs to improve the trustworthiness and reliability of electronic parts. Three main programs include Trusted Integrated Circuits (TRUST), Integrity and Reliability of Integrated Circuits (IRIS), and Supply Chain Hardware Integrity for Electronics Defense (SHIELD). TRUST focused on a metrics based approach where contractors would determine the probability of detection versus the probability of false alarms. This method considered all changes to the IC, not only malicious attacks (DARPA TRUST, 2015).

Due to globaliztion of the IC market, many companies have shifted their production lines to offshore foundries. This shift has led to a lack of regulation that opens a door for malicious attacks and counterfeit ICs to be integrated into a design that do not meet performance and reliability specifications. IRIS seeks to develop new techniques that will non-destructively derive the function of digital, analog, and mixed-signal ICs. Also, the program "will produce methods of device modeling and analytic proccesses to

determine the reliability of an IC by testing a limited number of samples" (DARPA IRIS, 2015).

The surge in counterfeit parts has raised the question of security and integrity of electronic systems in the DOD. The DARPA SHIELD program focuses on creating a new anti-tamper "dielet" that can be inserted into the package of an IC. The dielet will act as identification as well as detect any attempt to access or reverse engineer the dielet (DARPA SHIELD, 2015).

The focus on open foundaries and supply chain assurance is addressed in the Intelligence Advanced Research Projects Activity (IARPA) Trusted Integrated Chips (TIC) program. The concept of TIC is to create a split-manufaturing that allows both the academic world and US industries to have open access to design high performance ICs while still maintaining the quality and protection throughout the fabrication and intellectual properties (McCants, 2015).

Another technical measure that can be utilized is scanning a parts electromagnetic (EM) signature. Every part emits a unique EM signature similar to that of a human fingerprint. The same types of parts will have similar signatures, but with a natural variation induced from fabrication. Major variations in the signatures are indications that the part could be recycled, damaged, have a different fabrication process, or in more severe circumstances tampered with. The following section goes into more detail on EM signatures and how it is pertinent to this research.

Electromagnetic Emissions and Signatures

EM fields are produced through normal current fluctuations during circuit operation. Tiny process variations induce a slightly different emission to make a distinctive signature. There are two types of radiated emissions, (1) intentional radiated emission (IRE) and (2) unintetnional radiated emission (URE). There has been a multitude of research efforts in the form of RF emissions over the years (Cicchiani, Hartmuller and Sell, 2008; Montanari, Tacchini and Maini, 2008; Boyer, Ndoye and Dhia, 2009; I. Montanari, 2005; Boyer, Dhia and Li, 2013; DiBene II and Knighten, 1997; Muccioli, North and Slattery, 1997; Cobb, Lapse and Baldwin, 2011; Cobb, Garcia and Temple, 2010). Much emphasis has been placed at the device or integrated circuit level and at a low frequency (below 1 GHz). Research has shown that stress on these parts--whether temperature, voltage, accelerated life tests, or aging--affect the EM signature. The EME can often show the signs of aging or failures in a system. Research completed at the device level determined some of the main failure mechanisms include time dependent dielectric breakdown (TDDB), hot carrier injection (HCI), and negative bias temperature instability (HBTI).

Radio frequency distinct native attribute (RF-DNA) fingerprinting is a new way to identify embedded ICs through the collection of unintentional RF emissions (Cobb et al., 2010). This leaked information allows operational details of the device performance and data processing to be inferred (Cobb et al., 2011). The collection of EME is completed with the use of a near-field probe connected to an oscilloscope or a spectrum analyzer, depending on the specific type of test. At times, an anechoic chamber is utilized

to exclude an environmental emissions that would interfere (EMI) with the device or unit under test (DUT or UUT).

Nokomis Inc. has recently developed a system to identify counterfeit electronic parts through a part's URE. The Advanced Detection of Electronic Counterfeits (ADEC) system uses an ultra-sensitive Hiawatha receiver to form the core of the system. It currently has a database of 90 different types of parts from 6 distributors. ADEC uses a part's URE to identify the part's authenticity within a 5 second measurement. The system is still under development (Pathak and Keller, 2013).

APREL EM-ISight Tool

APREL is a Canadian-based company that originated with the development of an automated Specific Absorption Rate (SAR) test system in 1999 for near field measurements. SAR is a measure of the amount of RF energy absorbed by the body, often from a cell phone. In 2011 they released the EM-ISight system which is a flexible EMI/EMC (electromagnetic compatibility) measurement system. It performs near-field EM scans of a DUT to produce a 3-D representation of the field spectrum across the board. Common applications include EMI noise emission analysis, shield placement, design optimization, and possible susceptibility. Measurements are taken using either an E or H-field probe that acts as an antenna to collect the EMEs. A spectrum analyzer is connected to the LNA which interfaces with the EM-ISight system. The advanced software is used for setting up the test plan, automating data collection over a specified spectrum, and post-test data analysis. Figure 3 provides a block diagram of the EM-ISight system.

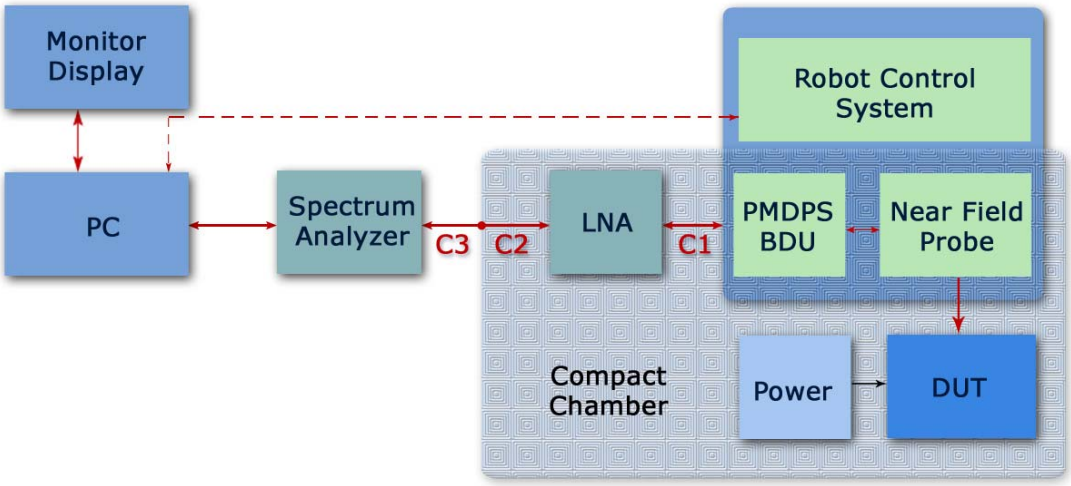


Figure 3 EM-ISight Block Diagram

In this research, the EM-ISight tool is employed to take measurements at the circuit level. A DOE is established and conducted to optimize the set of scanning parameters to return the best responses for the test. The Methodology section below will describe details of the individual tests conducted.

Summary

Chapter II summarized several topics of interest for this research. It investigated the statistics and impacts of counterfeit items on the economy. From there, a variety of detection and avoidance methods were examined to prevent the implementation of corrupt parts into major systems. Finally, EM signatures and their susceptibility to stressful testing and aging were researched. Several methods focused on the failure mechanisms at the device level. These previous research topics are the foundation for this research to detect counterfeit items through an EM signature that signifies aging, failure mechanisms, or counterfeit parts implemented at the board level.

III. Methodology

Chapter Overview

The purpose of this chapter is to define the test methodology used to develop a DOE, collect data, and analyze the overall sensitivity of the system and the average process variations of the selected devices. The test equipment, selected device, and descriptions of what each test is composed of is defined and described in this chapter.

Test Equipment

Several systems and COTS software are used in this research. The APREL EM-ISight is comprised of a Denso robotic arm, a Denso robot controller, a boundary detection unit (BDU) attached to the arm, an E or H-field probe attached to the BDU, a low noise amplifier (LNA), a working base with device restraints, a validation micro-stripline, a laptop that uses the EM-ISight V4.4 software, and various cables as shown in Figure 4. The majority of this equipment is enclosed in an anechoic chamber to reduce the effects of emissions of stray charges from other lab equipment.

The APREL software allows the user to setup a test routine for the device under test (DUT) and automatically control the robotic arm to move throughout the X, Y, Z, and theta positions. The software collects the spectrum of data through communication with a Tektronix spectrum analyzer, model RSA6120A. Once all the data is collected the software features a data analysis capability to complete any post-processing analysis, including noise floor elimination and a comparative scan application to determine the differences between two identical scans. A Wiltron signal generator, model 68159B, is used for daily validation at a manufacturer calibrated frequency, in coordination with the

appropriate probe and micro-stripline. The validation process is described in more detail in the Test Setup section below.

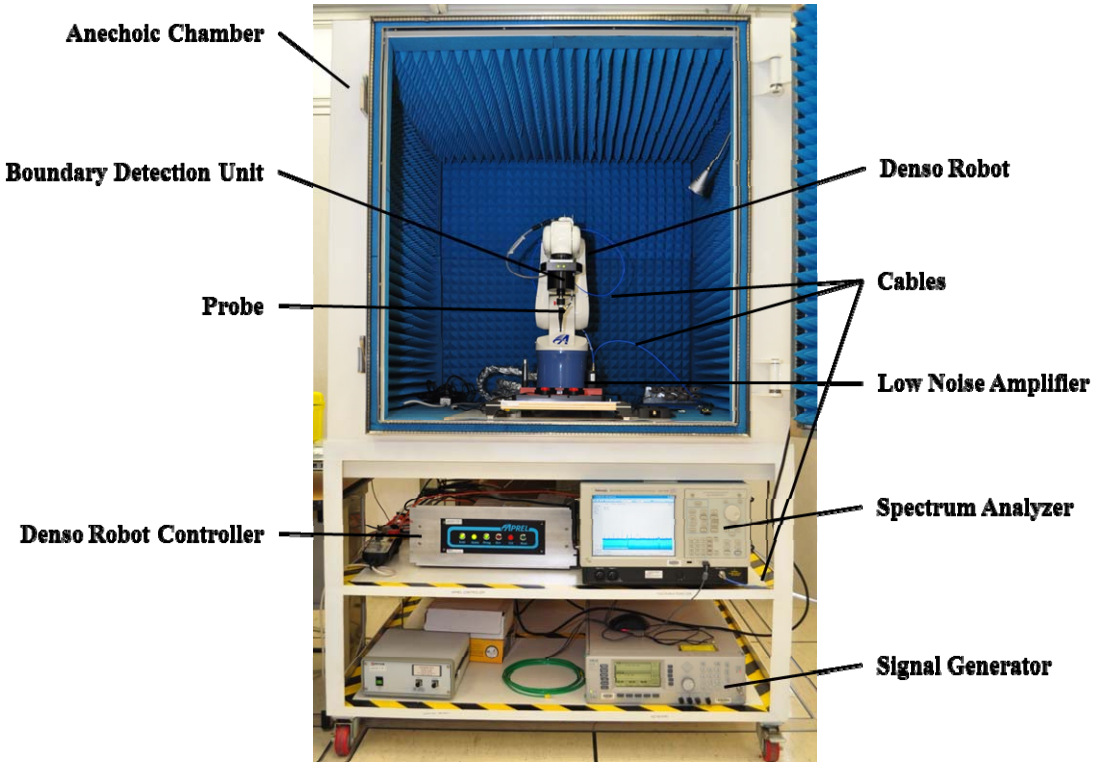


Figure 4 Aprel EM-ISight Test Setup (Front View)

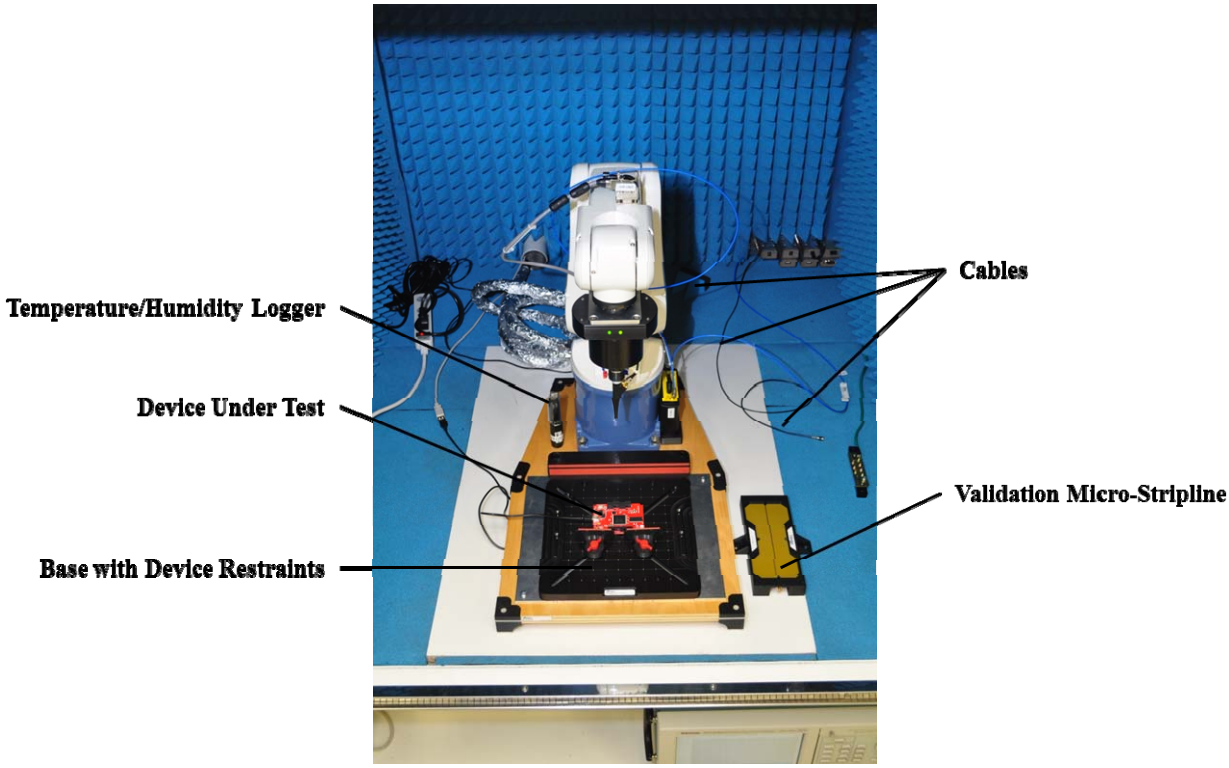


Figure 5 Aprel EM-ISight Test Setup (Top View)

Test Setup

The test setup is composed of several components including the system validation, board placement, and probe location reference in addition to the system setup described above. A system validation is done daily using the probe of interest at one of the specified frequencies recommended by the manufacturer. 300 MHz is the closest calibrated frequency that matches the center frequency for these tests and was used for all the system validations. Figure 5 shows these components utilized for the tests.

After system validation, the test article is attached to the base unit to prevent it from moving during testing. The base unit was fabricated with threaded holes, at equally spaced intervals, in order to attach test articles directly to the base. Two of these holes, in

the base, line up directly with two corners of the board selected for testing in this research. Those two corners are screwed into the base unit to ensure stability. In addition to the two corners attached directly to the base unit, the opposite side is held in position with two adjustable device restraints. To ensure consistent physical placement of the multiple boards, the same two holes are used every time. By using the same holes to attach the different boards, the location of interest should not move. This allows for consistency of the physical test area and probe placement. For every test, the probe needs a reference location in the bottom left hand corner. This reference allows for the same test area to be used for all the scans, despite the spatial resolution. Finally, the whole suite of tests can be measured. More details on the suite of tests are described in the following sections.

Device Under Test (DUT)

The device of interest is a Xilinx Spartan-6 FPGA chip housed on a Papilio Pro circuit board. This silicon-based device is a COTS product so it is cost-effective, easy to use, and offers the user the flexibility of reprogramming the device to induce a specific change. In this research, change is induced by alternating the programmed frequency from 305 MHz, using three inverters, to a frequency of 225 MHz, using 5 inverters. Figures 6 and 7 depict the Papilio board with Spartan-6 FPGA. Both the packaged and X-ray image are portrayed.

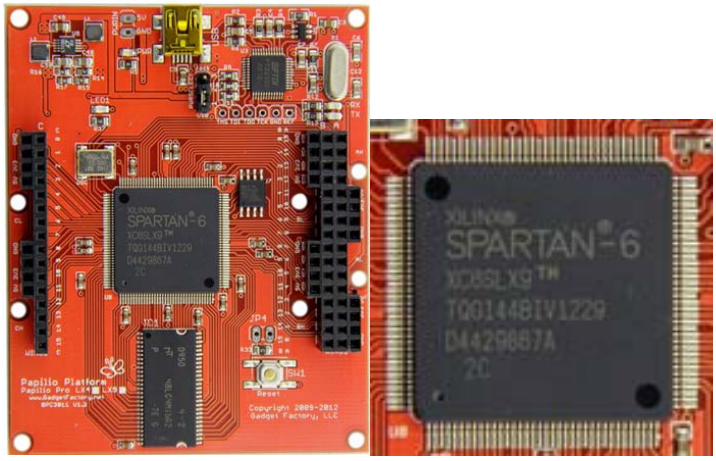


Figure 6 Papilio Pro Circuit Board with Xilinx Spartan-6 FPGA (Gadget Factory, 2015)

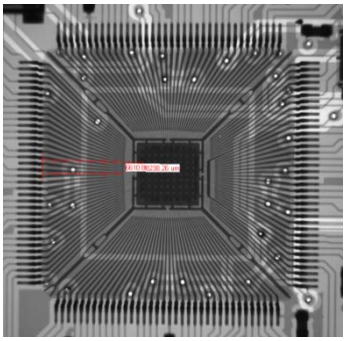


Figure 7 Xilinx Spartan-6 FPGA X-Ray image taken by Steve Tetlak (AFRL/RYDD, 2015)

Twelve boards were purchased to complete the various test routines described in the following sections, one of which was damaged on arrival from the manufacturer and was not be used for testing. The micro-USB adapter was damaged and the part could not be turned on or programmed. This part was used as a practice part for the etching process. Table 1 describes the allocation of devices for each test. The number of devices was selected based on the real-world application and constraints (time, money, and resources) of this project in the laboratory environment. The sample size is not large enough to be statistically significant, but this is what resources were allocated for this project. To achieve statistically significant data ($\alpha = 0.05$) and assuming an effect size of large with a power of 0.80, the minimal sample size would be 26 devices as shown in Table 2 from

Cohen's "A Power Primer" (Cohen, 1992). With the current sample size of 11, for the process variation test, the experiment will only have a power of approximately 0.43 rather than the recommend 0.80 as noted at the top of Table 2.

Table 1 DUT Allocation

Device ID	DOE	Process Variation Test	Sensitivity Test	Etched Test
Device 1		X		
Device 2		X		
Device 3		X		
Device 4	X	X		
Device 5		X		
Device 6		X		
Device 7		X	X	
Device 8		X		
Device 9		X		
Device 10		X		X
Device 11		X		
Device 12		**Damaged**		

Table 2 Minimal sample size based on effect size, power, test, and α. (Cohen, 1992)

Table 2
N for Small, Medium, and Large ES at Power = .80 for α = .01, .05, and .10

	α								
	.01			.05			.10		
Test	Sm	Med	Lg	Sm	Med	Lg	Sm	Med	Lg
1. Mean dif	586	95	38	393	64	26	310	50	20
2. Sig *r*	1,163	125	41	783	85	28	617	68	22
3. *r* dif	2,339	263	96	1,573	177	66	1,240	140	52
4. *P* = .5	1,165	127	44	783	85	30	616	67	23
5. *P* dif	584	93	36	392	63	25	309	49	19
6. χ^2									
1*df*	1,168	130	38	785	87	26	618	69	25
2*df*	1,388	154	56	964	107	39	771	86	31
3*df*	1,546	172	62	1,090	121	44	880	98	35
4*df*	1,675	186	67	1,194	133	48	968	108	39
5*df*	1,787	199	71	1,293	143	51	1,045	116	42
6*df*	1,887	210	75	1,362	151	54	1,113	124	45
7. ANOVA									
2*g*[a]	586	95	38	393	64	26	310	50	20
3*g*[a]	464	76	30	322	52	21	258	41	17
4*g*[a]	388	63	25	274	45	18	221	36	15
5*g*[a]	336	55	22	240	39	16	193	32	13
6*g*[a]	299	49	20	215	35	14	174	28	12
7*g*[a]	271	44	18	195	32	13	159	26	11
8. Mult *R*									
2*k*[b]	698	97	45	481	67	30			
3*k*[b]	780	108	50	547	76	34			
4*k*[b]	841	118	55	599	84	38			
5*k*[b]	901	126	59	645	91	42			
6*k*[b]	953	134	63	686	97	45			
7*k*[b]	998	141	66	726	102	48			
8*k*[b]	1,039	147	69	757	107	50			

Note. ES = population effect size, Sm = small, Med = medium, Lg = large, diff = difference, ANOVA = analysis of variance. Tests numbered as in Table 1.
[a] Number of groups. [b] Number of independent variables.

Test Routines

A brief description of the test routines was mentioned in the previous section as it applies to the particular device(s) and sample size. Below is a block diagram that illustrates the testing process for this research. Each of the blocks is described in more detail below.

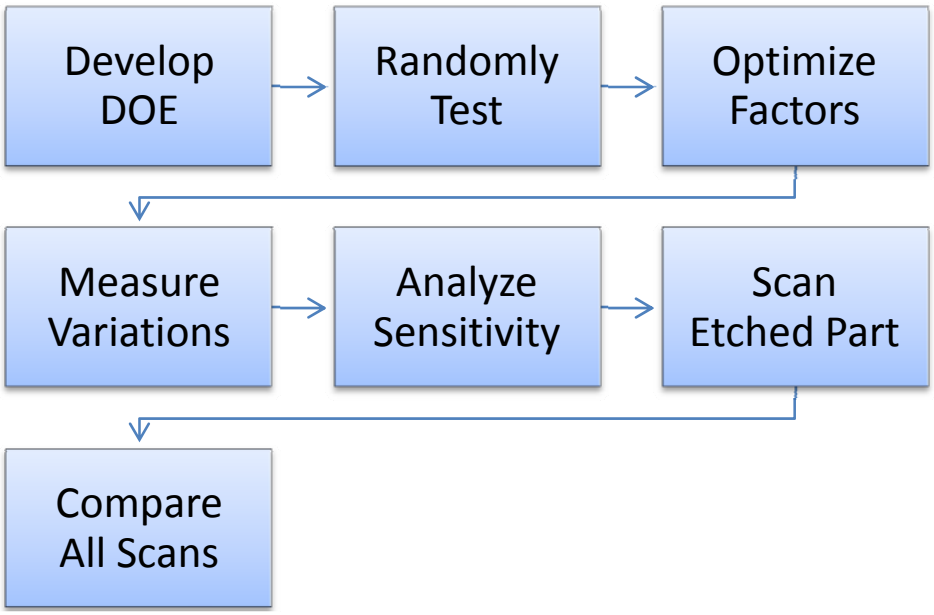


Figure 8 Test Routine Block Diagram

Develop DOE

The initial step in this multi-step process is to develop a DOE including all the independent and dependent factors. For this set of experiments there are five independent factors, each with two levels, and there are two dependent factors. The five independent factors are probe type, Z-height, spatial resolution, frequency range, and resolution bandwidth (RBW). There are two probe types, E and H-field probes. Past experience has indicated that a scan using the E-field probe portrays more of the functionality of the device, as opposed to a scan with an H-field probe which depicts more of the operational aspects of the circuit. The Z-height varied between 1 mm and 5 mm above the device

depending on the test. Spatial resolution refers to the X, Y-grid spacing over the device; the smaller the resolution, the more points that were measured over the device area. The spatial resolution varied between 0.2 mm and 1 mm over the device depending on the test. The frequency range describes the total frequency spectrum range with the center point of 300 MHz. The two levels for the frequency range are 100 MHz and 500 MHz depending on the test. The incremental spacing used in frequency range refers to the RBW. The RBW is typically automatically set to 10 kHz, but for this set of tests it will vary from 100 Hz to 10,000 Hz (10 kHz). The independent factors and their levels are listed in Table 3.

Table 3 Independent Factors and Levels

Independent Factor	Low Level	High Level
Probe	E-field	H-field
Z-Height	1 mm	5 mm
Spatial Resolution	0.2 mm	1 mm
Frequency Range	100 MHz	500 MHz
RBW	100 Hz	10,000 Hz

As mentioned previously, there are two dependent factors--peak programmed frequency and time of scan. Frequency magnitude measured in dBm0 is the key component of the peak programmed frequency and is the main response for the DOE. Several other components of the peak programmed frequency are subjectively analyzed. These components include the peak programmed frequency, the peak's X, Y, Z spatial locations, and the width of that peak. The time of scan is measured in minutes from the time data collection starts at point 1 until it collects all the data at all points selected based on the test setup. The dependent factors are listed in Table 4.

Table 4 Dependent Factors

Dependent Factors	Component
Peak Programmed Frequency	Magnitude
Time of Scan	Minutes

The DOE consists of five factors (the five independent factors) at two levels each. A full, half, and quarter factorials are all viable options, but based on the constraints noted above and due to the objective of identifying those factors with large effects, a half fractional factorial (2^{5-1}) design with center points is sufficient for this DOE. Screening experiments such as this are typically performed in the early stages of a project to determine significant factors. The center points are included as a checking mechanism throughout the DOE and eliminate the assumption of linearity.

Randomly Test

A total of twenty tests were established in the DOE, sixteen from the half fractional factorial design plus four center points. The run order was randomized to eliminate potential bias or day-to-day variations. Randomizing the experiments allows for more reliable and valid data. Table 5 shows the randomized test order used for this research. The four center points are scattered throughout the test sequence of the DOE to check for consistency. For the DOE, the FPGA is programmed as a ring oscillator at a frequency of 305 MHz, using 3 inverters to act as a point source. Two nuisance factors were defined in this research – room temperature and humidity. These factors may have an effect on the response, but are not controlled. Therefore, the ambient values were monitored throughout the various tests with a temperature/humidity data logger. Their effects are outside the scope of this research effort, and were noted as nuisance factors.

Table 5 DOE Test Order and Sequence

RunOrder	StdOrder	Probe	Z-Height (mm)	Spatial Resolution (mm)	Frequency Range (MHz)	RBW (Hz)
1	16	H	5	1	1000	10000
2	19	E	3	0.6	750	5000.5
3	4	H	5	0.2	500	10000
4	20	H	3	0.6	750	5000.5
5	3	E	5	0.2	500	1
6	13	E	1	1	1000	10000
7	2	H	1	0.2	500	1
8	5	E	1	1	500	1
9	8	H	5	1	500	1
10	11	E	5	0.2	1000	10000
11	1	E	1	0.2	500	10000
12	7	E	5	1	500	10000
13	18	H	3	0.6	750	5000.5
14	14	H	1	1	1000	1
15	10	H	1	0.2	1000	10000
16	17	E	3	0.6	750	5000.5
17	6	H	1	1	500	10000
18	15	E	5	1	1000	1
19	9	E	1	0.2	1000	1
20	12	H	5	0.2	1000	1

*Center points are highlighted gray.

Optimize Factors

After the data are collected for the DOE designed above, all factors and responses are analyzed (described in Chapter IV). From the gathered data, significant factors are determined. Then the factors can be optimized to produce the desired responses based on this DOE. Ideally, the optimized factors will produce a high magnitude peak programmed frequency in a short scan time. Means and standard deviations of the peak programmed frequency are calculated from the various scans.

Measure Variations

With the optimization of the factors, the process variations between the 11 boards can be scanned and compared. Once again the FPGA is programmed as a ring oscillator at a frequency of 305 MHz. Subtle changes in the signature can be attributed to basic fabrication practices that create a unique fingerprint for each device. Extreme variations can be linked to a process defect, a counterfeit device, or an indication of tampering. Overall, this can be used as a designator that the part should not be used in the end system. The means and standard deviations of the different boards are calculated to account for the normal process variation. This is an important feature that is fed forward in the next test routine.

Analyze Sensitivity

After the average process variation was calculated from the tests described above the FPGA was reprogrammed (still as a ring oscillator), by using a different number of inverters (5 instead of 3) to adjust the frequency from 305 MHz to 225 MHz. This value was selected in order to be outside the range of the natural manufacturing variance.

Scan Etched Part

The final part tested was a board that had part of the packaging etched away in order to expose the die and bond wires. Another scan with the optimized factors and the original programming as a ring oscillator at 305 MHz is completed. The purpose of this scan is to determine if the package provides any shielding that may lower the magnitudes or narrow the widths of any frequencies.

X-ray images were taken using an Xradia (now Zeiss) Micro XCT200. Figures 9 and 10 display the X-ray 2-D and 3-D images of the FPGA. The 2-D image had a 30 second exposure with 150 kV source and a 10 W beam energy. The 3-D image had the

same parameters, but it was averaged three times from -91 to 91 degrees. The 3-D scan took approximately 6 hours. Silver paint had to be added to the top of the package to act as an absorbing coat in order to clearly see the epoxy package surface. The epoxy package could not be seen in the original scan due to all the peripheral circuitry. Also, cable connectors absorbed too much of the low energy X-rays, that usually would have been absorbed by the mold compound. Figure 11 shows the relative measurement from the top of the wire bond to the backside of the package to be approximately 150 um. This is the distance that must be etched through to expose the bond wires.

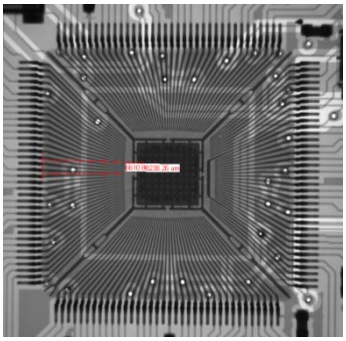


Figure 9 Xilinx Spartan-6 FPGA top view X-Ray image taken by Steve Tetlak (AFRL/RYDD, 2015).

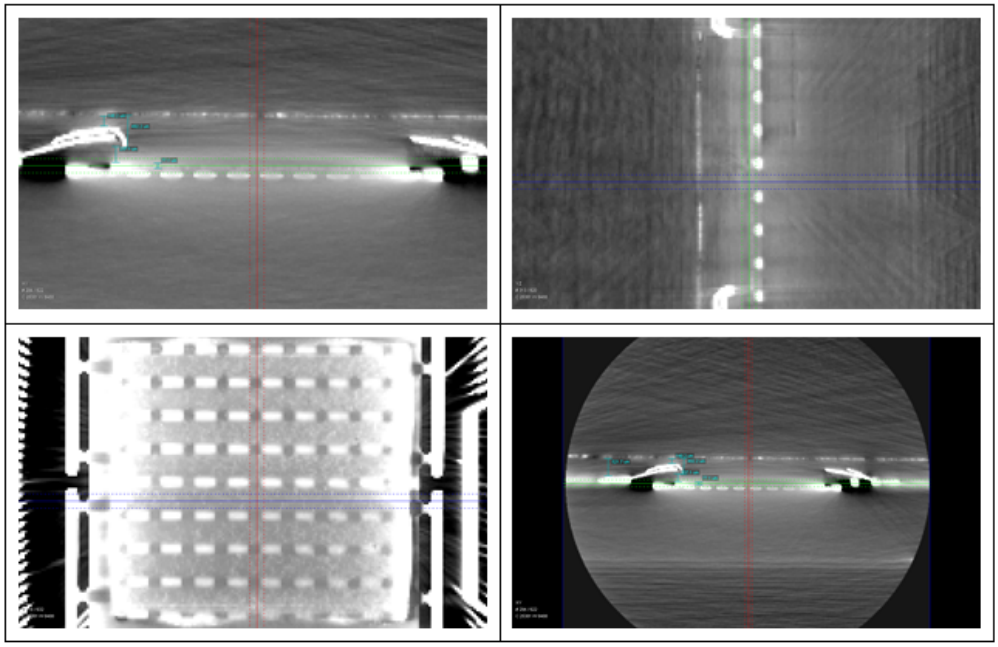


Figure 10 Xilinx Spartan-6 FPGA 3-D cross section X-Ray image taken by Steve Tetlak (AFRL/RYDD, 2015).

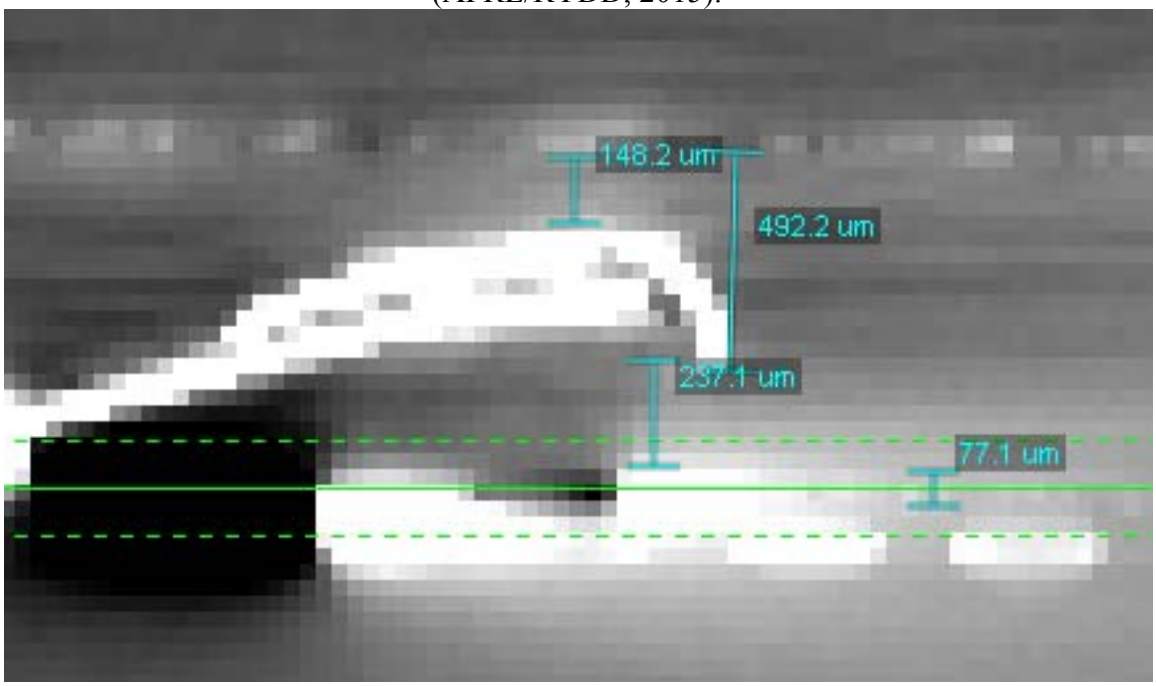


Figure 11 Xilinx Spartan-6 FPGA 3-D cross section measurement X-Ray image taken by Steve Tetlak (AFRL/RYDD, 2015)

The information from Figure 11 allows the process engineer to determine the parameters for the etching process. Board 12 (the damaged board) was originally used as

a practice board by the process engineer. This board was etched for 45 seconds in a nitric and sulfuric bath using a Nisene JetEtch II. This duration damaged the board beyond use. The second board, Board 10, was etched in the same nitric and sulfuric bath for only 10 seconds using a Nisene JetEtch II. The parameters of the etch were not optimized due to the limited number of samples available to refine the process. The center of the package was etched out to expose the die and the bond wires. Figure 12 displays the final outcome of the etching.

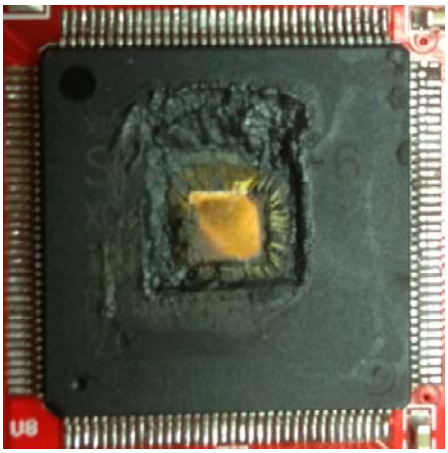


Figure 12 Xilinx Spartan-6 FPGA etched for 10 seconds (Etching performed by Jim Alverson, AFRL/RYDD, 2015).

Compare All Scans

After each set of tests, the scans were analyzed and compared to similar scans with matching conditions. The EM-ISight V4.4 software has a delta plot application that compares two scans taken at separate times, with the same test parameters (frequency range, spatial resolution, etc.) and creates an EM signature plot that displays the difference between the two scans. This feature is useful for determining variations in magnitude, location displacements, and frequency shifts throughout the spectrum. The

delta plots are used to analyze the differences in the programming for the sensitivity analysis and the difference in the shielding effects in the etched board test.

IV. Analysis and Results

Chapter Overview

This chapter discusses the application of the methodology and the results of the various tests outlined in Chapter III. Analysis of the responses from the DOE is completed to determine significant factors and their interactions. These factors are then optimized based on the desirability of each response. This optimization was used for the remainder of the tests including the process variation, sensitivity, and etched tests. Frequency and magnitude plots are illustrated for a visual representation of the responses on the FPGA. Frequency spectrums are used as well to depict the difference between tests.

DOE Test Results

Twenty tests were conducted over three days for the DOE. Two nuisance factors, temperature and humidity, were measured throughout this time period. These factors are depicted in Figure 13. The temperature varied between 70 and 80^{o}F while the relative humidity fluctuated between 40 and 50%. This small change in factors did not appear to have a significant effect on the DOE test responses. These responses are highlighted yellow in Table 6. The two responses measured for the DOE were the magnitude (dBm0) of the peak programmed frequency and the total time (minutes) taken to scan the entire FPGA. The magnitude plots are in dBm0. The magnitude units started as raw data (dBm) collected from the spectrum analyzer and then the EM-ISight software extracted all the losses and gains throughout the system as depicted in Figure 3 from Chapter II. This includes the probe coupling loss, LNA gain, BDU loss, cable losses (3 calbes total), and a

custom compensation factor for each manufacturer calibrated frequency. All of these were measured in dBm. Equation 1 calculates the the total dBm0 value for every measured point. For frequencies not included in the manufacturer's table, the software takes a linear interpolation between the two closes frequencies for the equation. A table of the calibrated frequencies for each probe can be found in Appendix B.

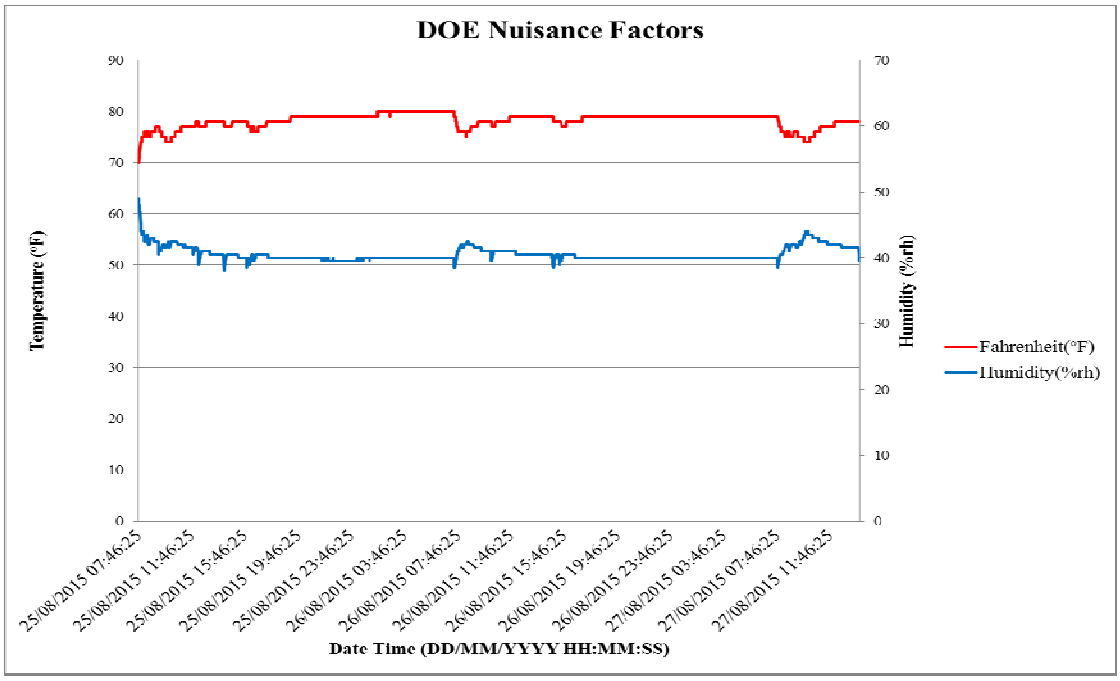


Figure 13 Plot of nuisance factors over DOE test period.

dBm0 = dBm - [Probe Coupling Loss (Vp_dBm)] - [LNA Gain] - [BDU Loss] - [Cable Losses (C1 to C3)] - [Custom Compensation Factors (K2 + K3)]
Equation 1 Calibrated Magnitude Value.

In addition to the two responses recorded in Table 6, several supplementary responses were documented. Table 7 encompasses these responses. It includes the number of peaks, the peak programmed frequency (MHz), that frequency's magnitude (dBm0), location (X, Y, Z), and the frequency width (MHz) for the programmed peak. The mean and standard deviation of each of these responses was calculated and is displayed in the last two rows of the table.

Table 6 DOE Responses

Run Order	Time Start	Time End	Probe	Z-Height (mm)	Spatial Res (mm)	Frequency Range (MHz)	RBW (Hz)	FreqMag (dBm0)	Scan Time (min)
1	806	816	H	5	1	500	10000	**-26.49**	**10**
2	823	845	E	3	0.6	300	5050	**-24.65**	**22**
3	954	1128	H	5	0.2	100	10000	**-26.51**	**94**
4	1140	1203	H	3	0.6	300	5050	**-22.23**	**23**
5	1207	1341	E	5	0.2	100	100	**-28.49**	**94**
6	1346	1356	E	1	1	500	10000	**-18.65**	**10**
7	1402	1538	H	1	0.2	100	100	**-16.21**	**96**
8	1545	1551	E	1	1	100	100	**-18.87**	**6**
9	1558	1603	H	5	1	100	100	**-27.01**	**5**
10	1618	2006	E	5	0.2	500	10000	**-27.76**	**228**
11	812	946	E	1	0.2	100	10000	**-18.49**	**94**
12	956	1011	E	5	1	100	10000	**-24.84**	**15**
13	1006	1028	H	3	0.6	300	5050	**-22.72**	**22**
14	1037	1047	H	1	1	500	100	**-16.59**	**10**
15	1051	1440	H	1	0.2	500	10000	**-16.11**	**229**
16	1446	1508	E	3	0.6	300	5050	**-22.98**	**22**
17	1513	1518	H	1	1	100	10000	**-16.79**	**5**
18	1523	1535	E	5	1	500	100	**-25.12**	**12**
19	1537	1926	E	1	0.2	500	100	**-17.72**	**229**
20	948	1336	H	5	0.2	500	100	**-26.37**	**228**

*Center points are highlighted gray.

Table 7 Supplementary DOE Responses

Run Order	Test Conditions	# Peaks	Prog Peak Freq (MHz)	Prog Freq Mag (dBm0)	Prog Freq Loc (X, Y, Z)	Prog Freq Width (MHz)
1	H, 5, 1, 500, 10000	18	306.25	-26.49	(13.99, 20, 5)	13.75
2	E, 3, 0.6, 300, 5050	15	307.5	-24.65	(13.79, 19.8, 3)	9.375
3	H, 5, 0.2, 100, 10000	6	307.375	-26.51	(14.21, 19.8, 5)	10.375
4	H, 3, 0.6, 300, 5050	12	306	-22.23	(13.79, 19.8, 3)	12.375
5	E, 5, 0.2, 100, 100	6	303.25	-28.49	(14.78, 6.4, 5)	10.75
6	E, 1, 1, 500, 10000	20	305.625	-18.65	(13.99, 20, 1)	10.625
7	H, 1, 0.2, 100, 100	7	305.875	-16.21	(13.79, 20, 1)	13.25
8	E, 1, 1, 100, 100	7	305.625	-18.87	(12.99, 19.99, 1)	9.75
9	H, 5, 1, 100, 100	7	307	-27.01	(14, 20, 5)	10.125
10	E, 5, 0.2, 500, 10000	20	303.125	-27.76	(19.02, 4.99, 5)	11.25
11	E, 1, 0.2, 100, 10000	6	306.375	-18.49	(13.39, 20, 1)	12.75
12	E, 5, 1, 100, 10000	6	303.375	-24.84	(16, 19.99, 5)	12.25
13	H, 3, 0.6, 300, 5050	13	306.375	-22.72	(13.81, 19.19, 3.01)	12.75
14	H, 1, 1, 500, 100	18	305.625	-16.59	(13.99, 20, 1)	13.75
15	H, 1, 0.2, 500, 10000	18	305.625	-16.11	(13.58, 20, 1)	13.75
16	E, 3, 0.6, 300, 5050	14	303.375	-22.98	(13.19, 19.8, 3)	12
17	H, 1, 1, 100, 10000	7	306.75	-16.79	(13.99, 20, 1)	13.125
18	E, 5, 1, 500, 100	18	303.125	-25.12	(14.99, 20, 5)	11.25
19	E, 1, 0.2, 500, 100	18	305.625	-17.72	(13.19, 20, 1)	10.625
20	H, 5, 0.2, 500, 100	18	306.25	-26.37	(13.79, 20, 5)	10.625
Mean		**12.7**	**305.50625**	**-22.23**	**(14.21, 18.5, 3)**	**11.725**
Standard Deviation		**5.58**	**1.45**	**4.36**	**(1.32, 4.39, 1.84)**	**1.42**

*Center points are highlighted gray.

Figure 14 shows an enlarged view of the frequency spectrum plots to show more detail. For viewing purposes, the frequency spectrums for the DOE tests are split into two figures, Figures 15 and 16. The frequency spans from 50 to 550 MHz with a center frequency of 300 MHz for the X-axis and -60 to 7 dBm0 for the Y-axis. There are several grayed out areas. These areas indicate a non-constant noise floor. For the E-field probe everything below 150 MHz is considered noise and for the H-field probe everything below 100 MHz is considered noise. Eliminating these areas allows for a more consistent noise floor and comparison of the peak magnitudes.

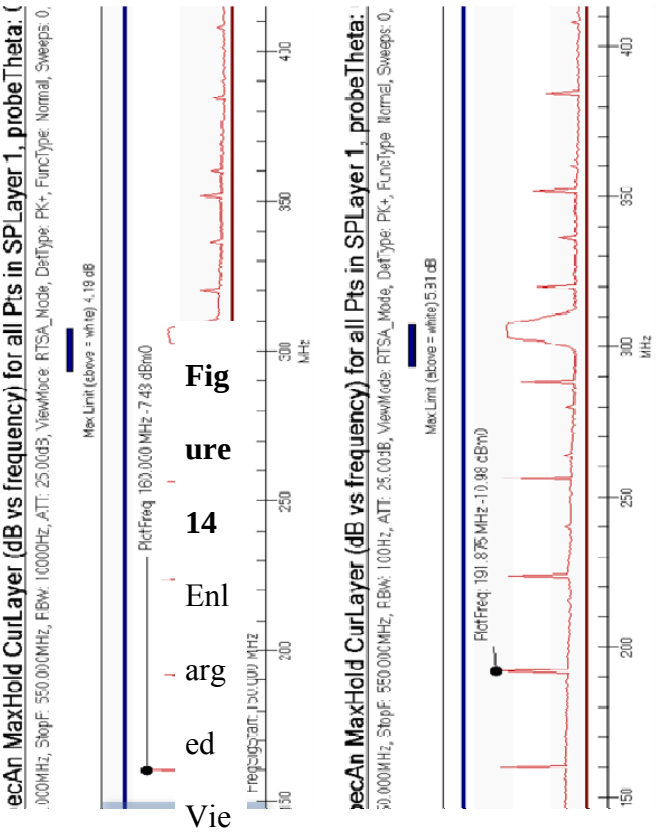


Figure 14 Enlarged View of E (T6) vs H

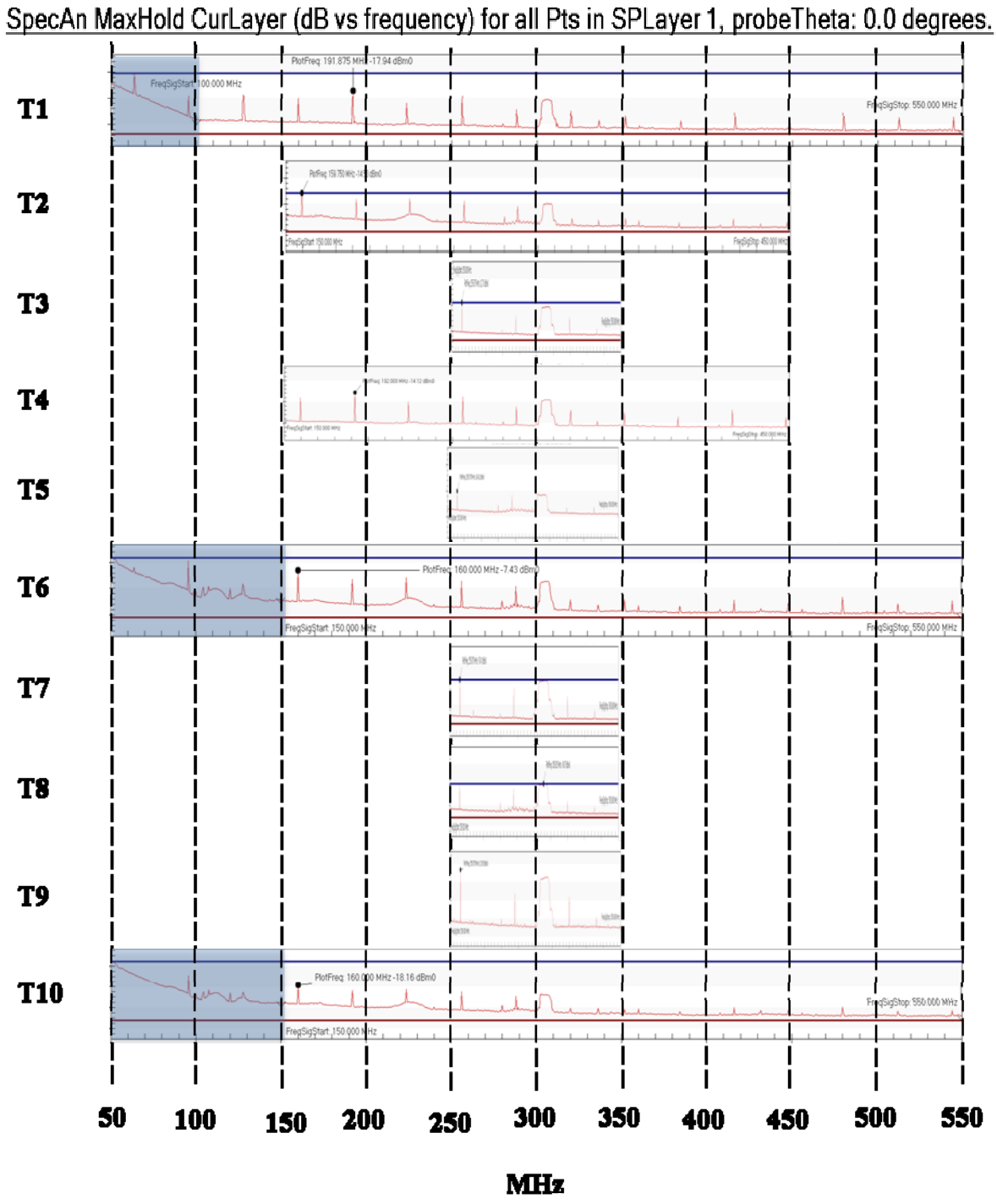


Figure 15 DOE Frequency Spectrum Tests 1-10

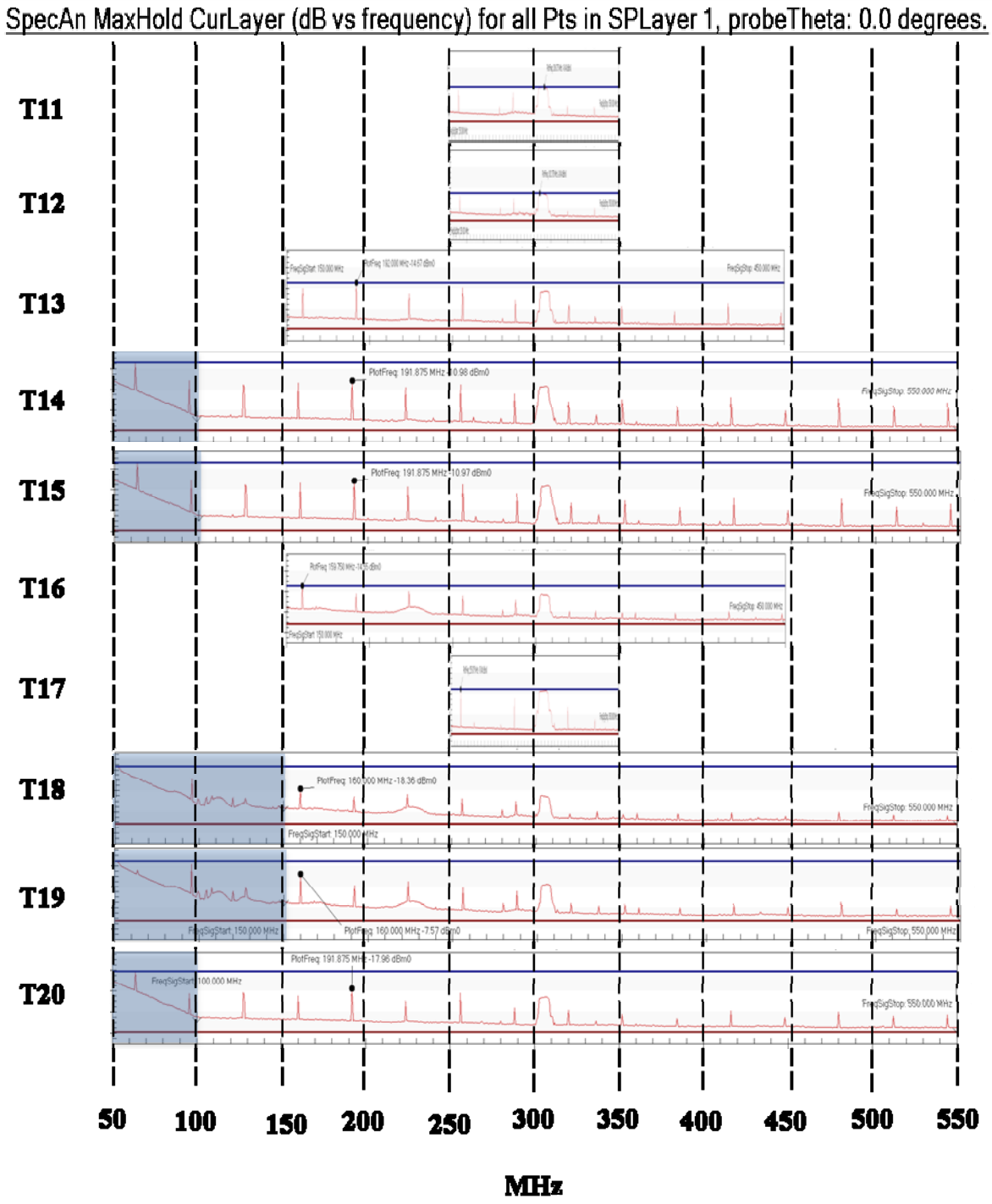


Figure 16 DOE Frequency Spectrum Tests 11-20

Figure 17 is an enlarged view of the frequency and magnitude plots, in order to show more detail. The plots on the left show the number of points used for the scan and in this case, the dimensions of the DUT as well since the spatial resolution was 1 mm. The plots on the right depict the APREL signatures overlaid on the X-ray image of the FPGA. In all the plots the blue dot or circle indicates the location with the highest magnitude.

Figures 18 and 19 represent the overall frequency and magnitude plots of the peak programmed frequency. The E-field tests show majority of the part radiating at the peak programmed frequency, whereas the H-field tests act as a point source that decreases in magnitude away from the point on the upper right edge of the device. The shape of the frequency plots vary between the E and H-field tests. The H-field tests have a funnel shaped design for the programmed frequency whereas the programmed frequency for E-field tests consume between 75-100 percent of the device. These unique map signatures can be a potential diagnostic tool for counterfeit electronic parts analysis.

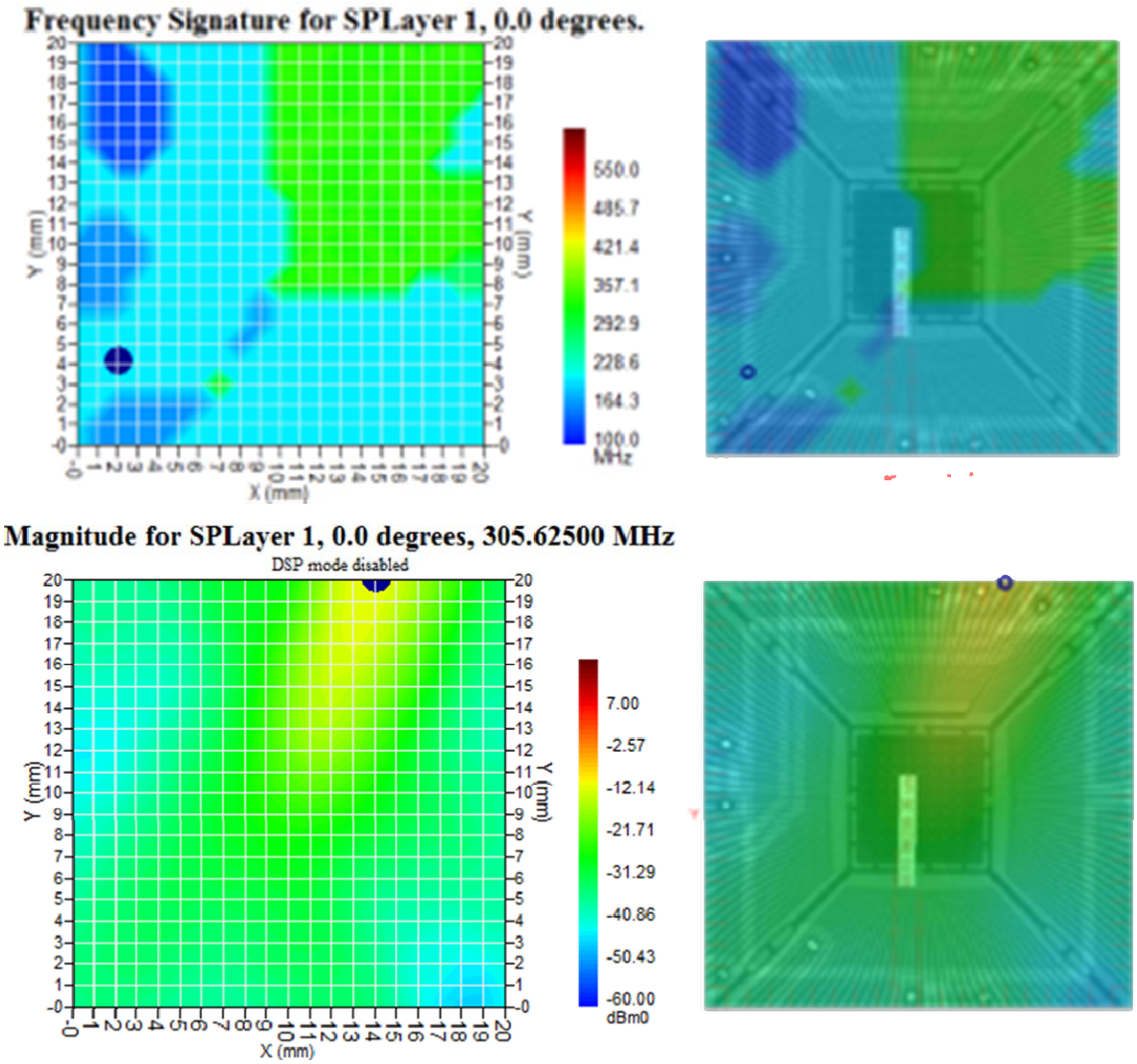


Figure 17 Enlarged Frequency and Magnitude Plots

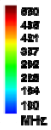
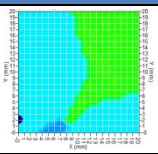
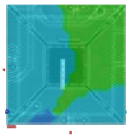
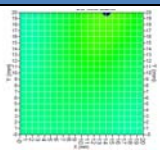
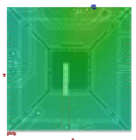
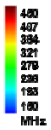
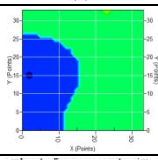
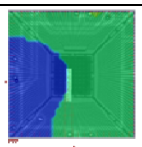
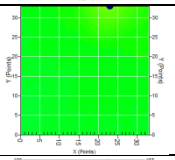
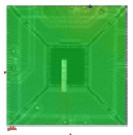
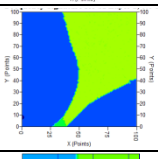
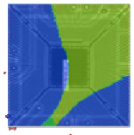
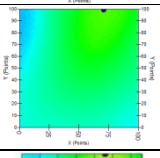
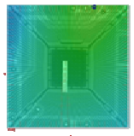
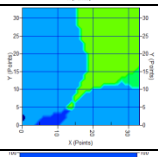
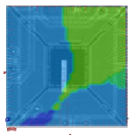
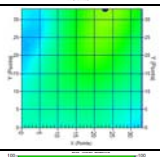
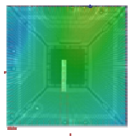
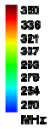
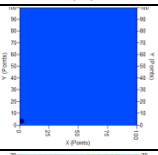
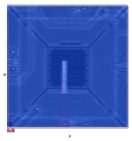
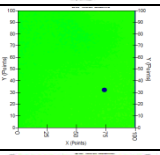
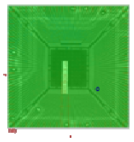
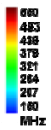
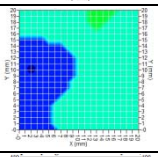
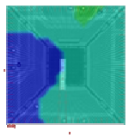
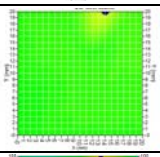
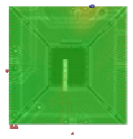
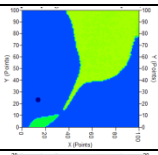
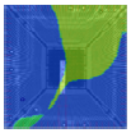
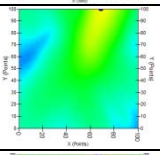
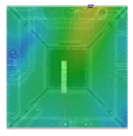
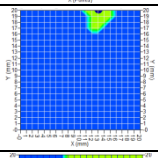
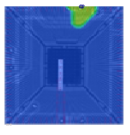
Test	Freq Range (MHz)	Freq (MHz)	Layered Freq (MHz)	Mag Range	Mag (dBm0)	Layered Mag (dBm0)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Figure 18 DOE Frequency and Magnitude Plots Tests 1-10

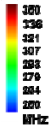
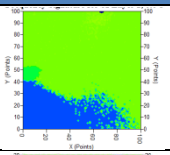
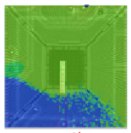
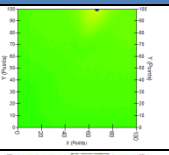
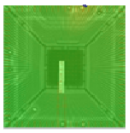
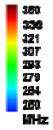
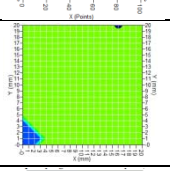
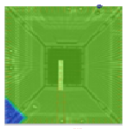
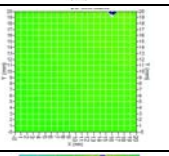
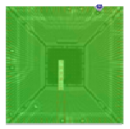
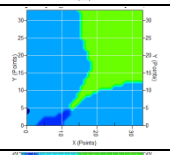
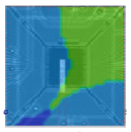
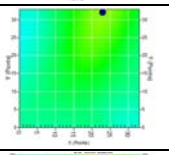
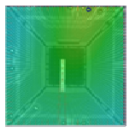
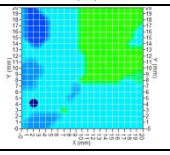
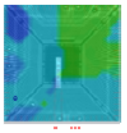
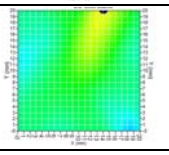
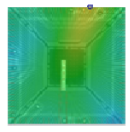
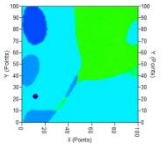
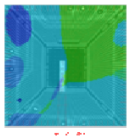
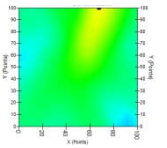
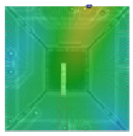
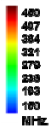
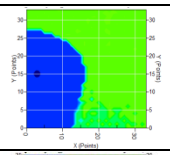
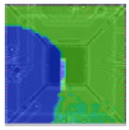
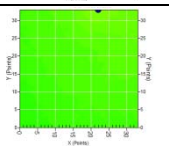
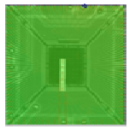
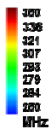
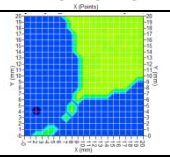
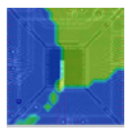
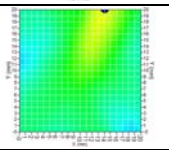
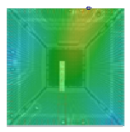
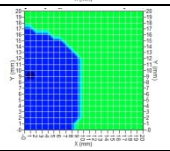
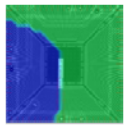
Test	Freq Range (MHz)	Freq (MHz)	Layered Freq (MHz)	Mag Range	Mag (dBm0)	Layered Mag (dBm0)
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

Figure 19 DOE Frequency and Magnitude Plots Tests 11-20

An analysis of variance (ANOVA) was computed for each response using JMP V10. The significant factors and interactions are shown in Figure 20 for the frequency magnitude response and Figure 21 for the scan time response. The only significant factor to effect frequency magnitude was the Z-height (outlined in red). This implies that a stronger signal is received through the probe when the probe is closer to the device. The signal strength decreases as the probe moves further away.

Response Freq Mag (dBm0)

Parameter Estimates

Term	Estimate	Std Error	t Ratio	Prob>|t|
Intercept	-22.23	0.269325	-82.54	<.0001*
Probe[H]	0.527	0.269325	1.96	0.1220
Z-Height(1,5)	-4.5725	0.301114	-15.19	0.0001*
Spatial Res (mm)(0.2,1)	0.20625	0.301114	0.68	0.5310
Freq Range (MHz)(100,500)	0.15	0.301114	0.50	0.6445
RBW (Hz)(100,10000)	0.04625	0.301114	0.15	0.8854
Probe[H]*Z-Height	-0.5125	0.301114	-1.70	0.1640
Probe[H]*Spatial Res (mm)	-0.41625	0.301114	-1.38	0.2390
Probe[H]*Freq Range (MHz)	-0.03	0.301114	-0.10	0.9254
Probe[H]*RBW (Hz)	-0.01125	0.301114	-0.04	0.9720
Z-Height*Spatial Res (mm)	0.5025	0.301114	1.67	0.1705
Z-Height*Freq Range (MHz)	-0.01125	0.301114	-0.04	0.9720
Z-Height*RBW (Hz)	0.1275	0.301114	0.42	0.6938
Spatial Res (mm)*Freq Range (MHz)	-0.0675	0.301114	-0.22	0.8336
Spatial Res (mm)*RBW (Hz)	0.05625	0.301114	0.19	0.8609
Freq Range (MHz)*RBW (Hz)	-0.4475	0.301114	-1.49	0.2114

Figure 20 Frequency Magnitude Response Significant Factor (JMP Output)

The scan time response also had one significant factor, but had another almost signifigant factor and interaction that is worth noting (outlined in blue). The spatial resolution (outlined in red) is the significant factor for the response time. Therefore, the more points measured, the longer the scan time. The frequency range is outside the 0.05 alpha value, but is the next significant factor after spatial resolution. The interaction of these two factors, spatial resolution and frequency range, also produce an almost significant response.

Response Scan Time (min)

Parameter Estimates

Term	Estimate	Std Error	t Ratio	Prob>|t|
Intercept	72.7	12.61414	5.76	0.0045*
Probe[H]	-0.5	12.61414	-0.04	0.9703
Z-Height(1,5)	0.4375	14.10304	0.03	0.9767
Spatial Res (mm)(0.2,1)	-76.1875	14.10304	-5.40	0.0057*
Freq Range (MHz)(100,500)	34.1875	14.10304	2.42	0.0724
RBW (Hz)(100,10000)	0.3125	14.10304	0.02	0.9834
Probe[H]*Z-Height	-0.8125	14.10304	-0.06	0.9568
Probe[H]*Spatial Res (mm)	-0.9375	14.10304	-0.07	0.9502
Probe[H]*Freq Range (MHz)	0.4375	14.10304	0.03	0.9767
Probe[H]*RBW (Hz)	-0.4375	14.10304	-0.03	0.9767
Z-Height*Spatial Res (mm)	0.9375	14.10304	0.07	0.9502
Z-Height*Freq Range (MHz)	-0.4375	14.10304	-0.03	0.9767
Z-Height*RBW (Hz)	0.6875	14.10304	0.05	0.9635
Spatial Res (mm)*Freq Range (MHz)	-32.8125	14.10304	-2.33	0.0805
Spatial Res (mm)*RBW (Hz)	0.5625	14.10304	0.04	0.9701
Freq Range (MHz)*RBW (Hz)	-0.5625	14.10304	-0.04	0.9701

Figure 21 Scan Time Response Significant Factor (JMP Output)

Because a factor and an interaction were close to being significant, another ANOVA was run with only three factors: Z-height, spatial resolution, and frequency range. There was no change in the magnitude response. The Z-height remained the only significant factor. However, running the ANOVA with three factors produced a different result for the scan time response. Figure 22 shows that there are two significant factors (spatial resolution and frequency range) and one significant interaction (spatial resolution * frequency range).This verifies that the frequency range and the interaction between the spatial resolution and frequency range are significant when the non-significant factors are taken out of the equation.

Response Scan Time (min)

Parameter Estimates

Term	Estimate	Std Error	t Ratio	Prob>|t|
Intercept	72.7	7.012167	10.37	<.0001*
Z-Height(1,5)	0.4375	7.839841	0.06	0.9563
Spatial Res (mm)(0.2,1)	-76.1875	7.839841	-9.72	<.0001*
Freq Range (MHz)(100,500)	34.1875	7.839841	4.36	0.0008*
Z-Height*Spatial Res (mm)	0.9375	7.839841	0.12	0.9066
Z-Height*Freq Range (MHz)	-0.4375	7.839841	-0.06	0.9563
Spatial Res (mm)*Freq Range (MHz)	-32.8125	7.839841	-4.19	0.0011*

Figure 22 Scan Time Response Significant Factors and Interactions with Only Three Factors (JMP Output)

After reviewing the significant factors, all the factors were optimized based on the response desirability. The desired response is measured on a scale from 0 (not desired) to 1 (desired). A higher frequency magnitude and a lower scan time are the desired outcomes for every scan. The optimization of the factors based on those desired outcomes is highlighted in red in Figure 23. These optimized settings are used for the remainder of the tests in this research. Those factor levels are the H-field probe, 1 mm Z-height, 1 mm spatial resolution, 500 MHz frequency range, and 100 Hz RBW.

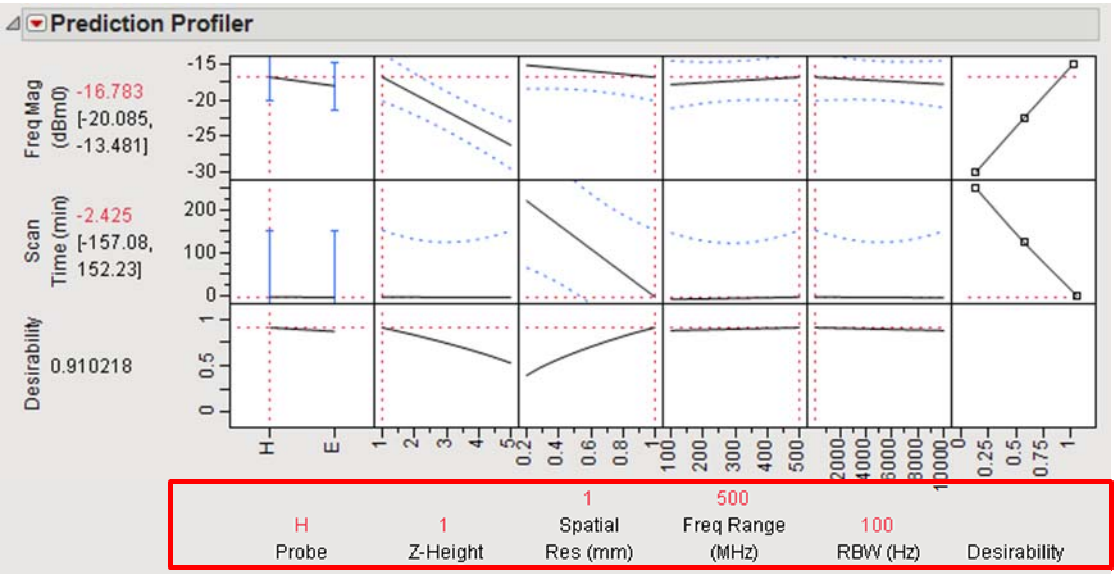


Figure 23 Factor optimization based on desirability

Process Variations Test Results

To determine the process variations, over the various boards, all the boards were tested using the optimized factor settings selected above. The results along with the means, differences, and standard deviations of these tests are located in Table 8. Board 1 and 12 did not work properly as demonstrated by the orange rows. Board 1 arrived in functional condition from the vendor and was programmed as a ring oscillator at a frequency of 305 MHz using three inverters. When the part was powered up to verify accurate programming, the programmed peak was at approximately 320 MHz. The signal shifted from 320 to 380 MHz over the course of a few minutes while the board warmed up. Once the board was powered down and turned back on, the programmed signal was gone altogether. The board was still scanned to show what a bad device looks like. Board 12 was delivered with a broken micro-USB connector. The board was never programmed and was used as a trial chip for the etching process, described in Chapter III.

Table 8 Process Variations Results Table

Board	Frequency (MHz)	Location (X, Y, Z)	Magnitude (dBm0)	Width (MHz)
1	**Bad Device**			
2	321.25	(13.99, 20, 1)	-13.42	15
3	306.25	(13.99, 19.99, 1)	-16.74	15
4	308.125	(13.99, 20, 1)	-15.91	13.75
5	311.25	(14, 20, 1)	-17.71	15
6	306.25	(13.99, 19.99, 1)	-17.15	11.25
7	310	(14.01, 18.98, 1.01)	-14.5	14.375
8	316.25	(13.99, 20, 1)	-14.62	15
9	312.5	(13.99, 20, 1)	-15.23	14.375
10	306.875	(12.99, 20, 1)	-16.77	14.375
11	301.875	(13.99, 19.99, 1)	-16.64	13.125
12	**Damaged**			
Mean	**310.0625**	**(13.89, 19.89, 1)**	**-15.869**	**14.125**
Difference	**19.375**	**(1.02, 1.02, 0.01)**	**4.29**	**3.75**
Standard Deviation	**5.59**	**(0.32, 0.32, 0.00)**	**1.38**	**1.19**

Table 8 shows the mean peak programmed frequency to be approximately 310 MHz, with a standard deviation of 5.59 MHz. Figure 24 depicts each board's peak programmed frequency magnitude with respect to the standard deviation. The blue box represents one standard deviation around the mean for both magnitude and frequency, yellow is two standard deviations and red is 3 standard deviations. Only one board (Board 2) was outside two standard deviations, three boards are within two standard deviations, and the rest are within one standard deviation.

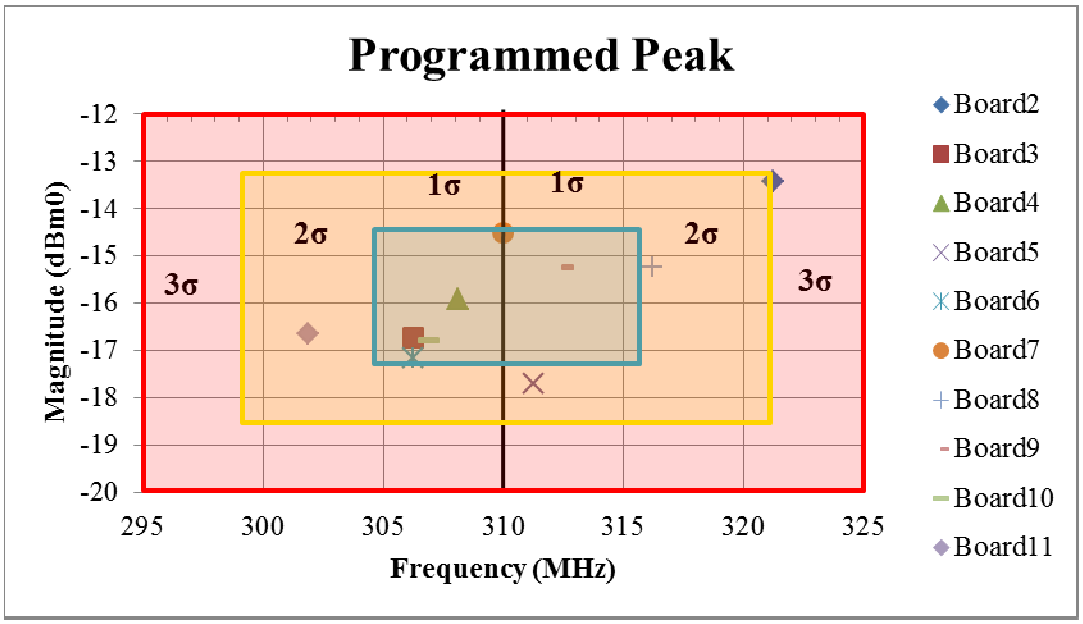


Figure 24 Programmed Peak Frequency and Magnitude by Board

Figures 25 and 26 display the consistency of peaks throughout the frequency spectrum with the exception of Board 1. As in the DOE, the frequency range from 50 to 100 MHz is grayed out to account for the rise in the noise floor. The area of interest, in the frequency spectrum, is in the black box highlighted yellow.

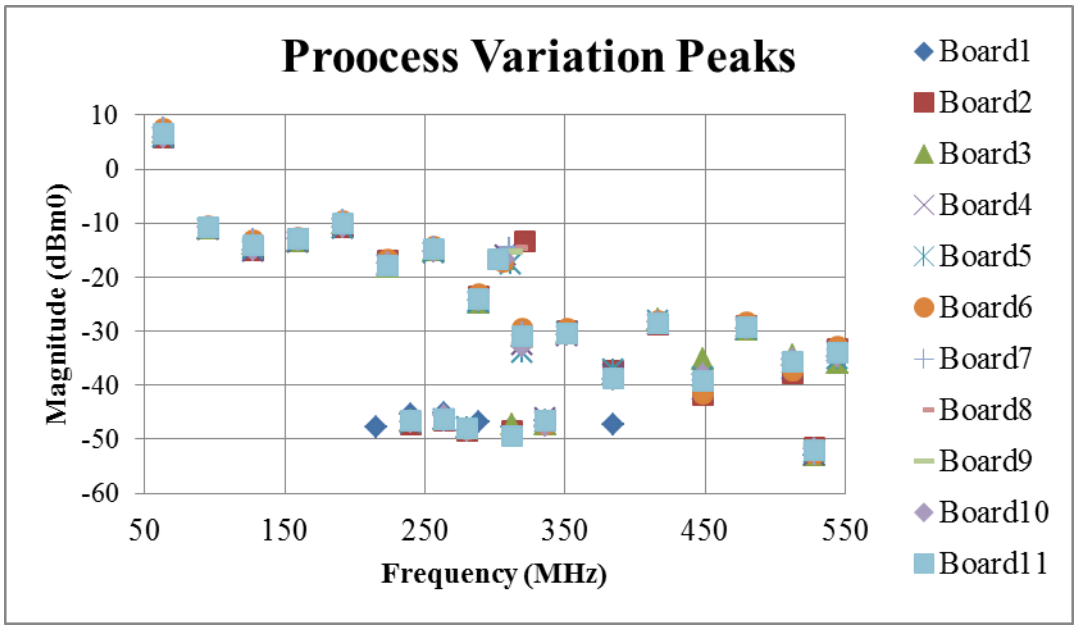


Figure 25 Programmed Peak Frequency and Magnitude by Board

Figure 27 illustrates the uniformity of the frequency and magnitude plots, with respect to location. The peak programmed frequency is located on the top right edge of the FPGA. That programmed frequency is also the dominant frequency for the upper right quadrant.

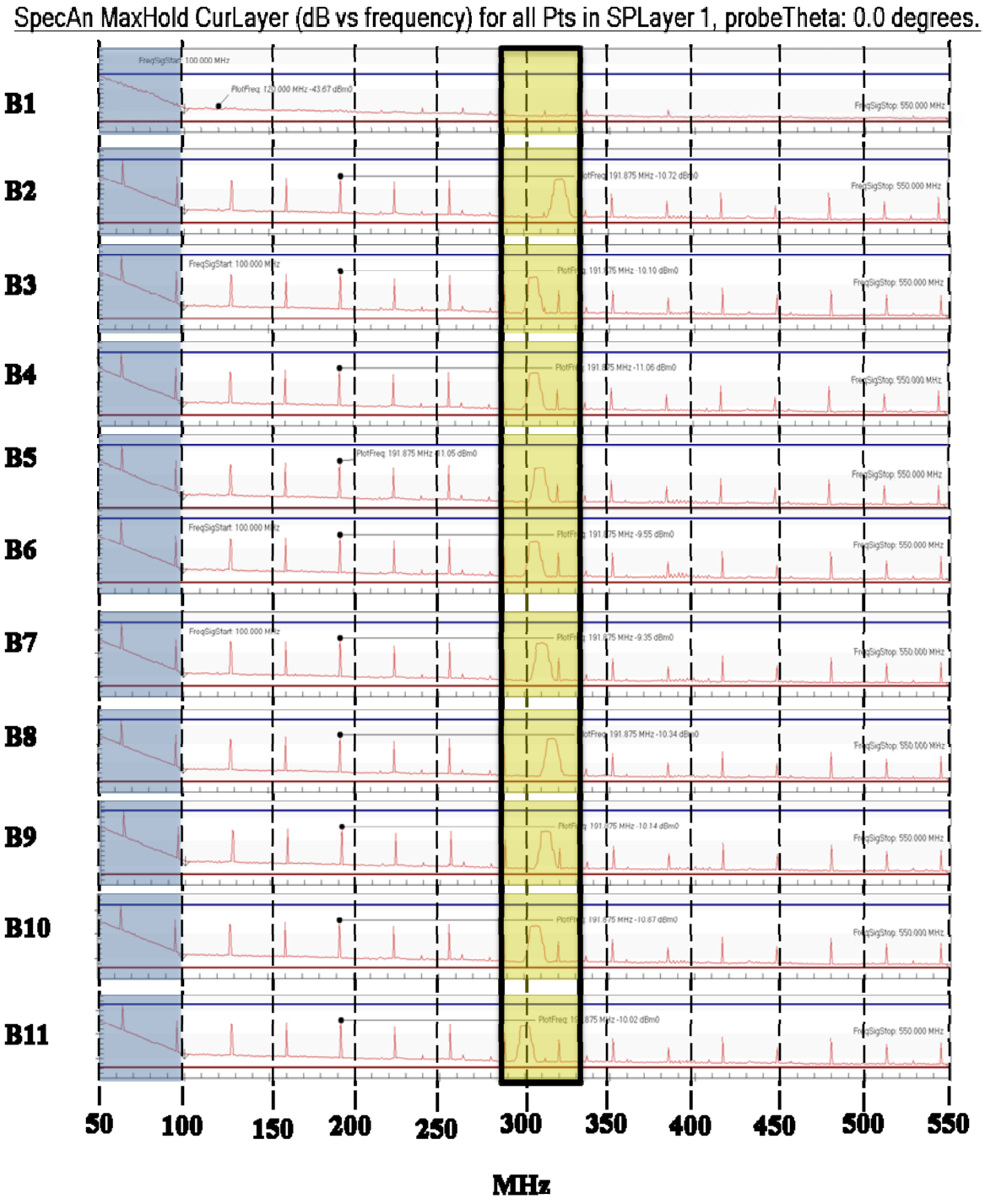


Figure 26 Process Variations Frequency Spectrum by Board

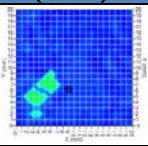
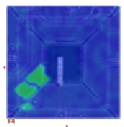
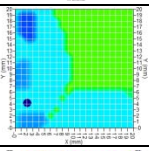
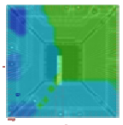
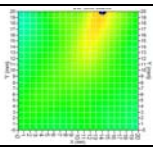
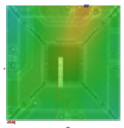
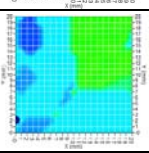
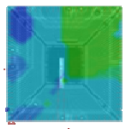
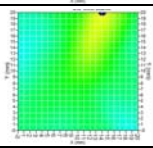
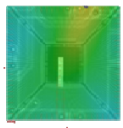
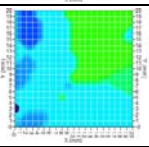
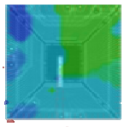
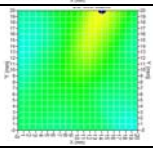
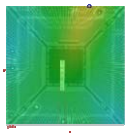
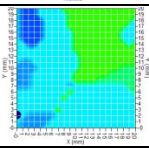
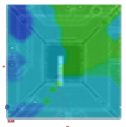
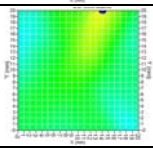
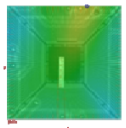
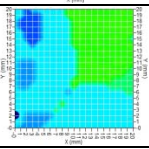
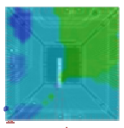
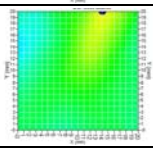
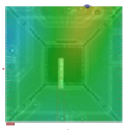
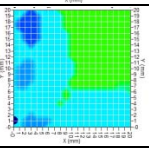
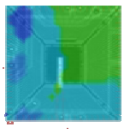
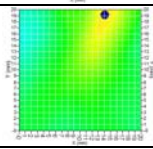
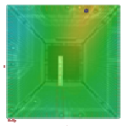
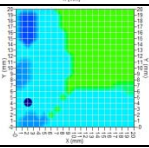
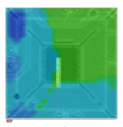
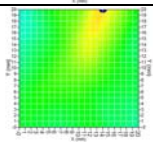
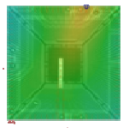
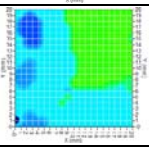
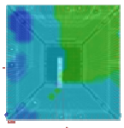
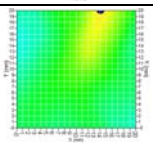
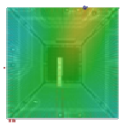
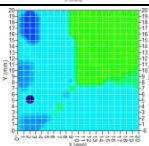
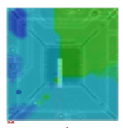
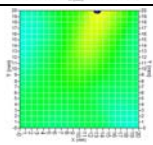
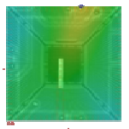
Board	Freq Range	Freq (MHz)	Layered Freq (MHz)	Mag Range	Mag (dBm0)	Layered Mag (dBm0)
1					N/A	N/A
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						

Figure 27 Process Variations Frequency and Magnitude Plots by Board

Once again, the temperature and humidity were measured throughout the tests to ensure consistent ambient settings. The temperature varied between 70 and 80°F, while the relative humidity fluctuated between 40 and 50%. These numbers are consistent with the DOE nuisance factors measured. This small change in factors does not appear to have a significant effect on the process variations.

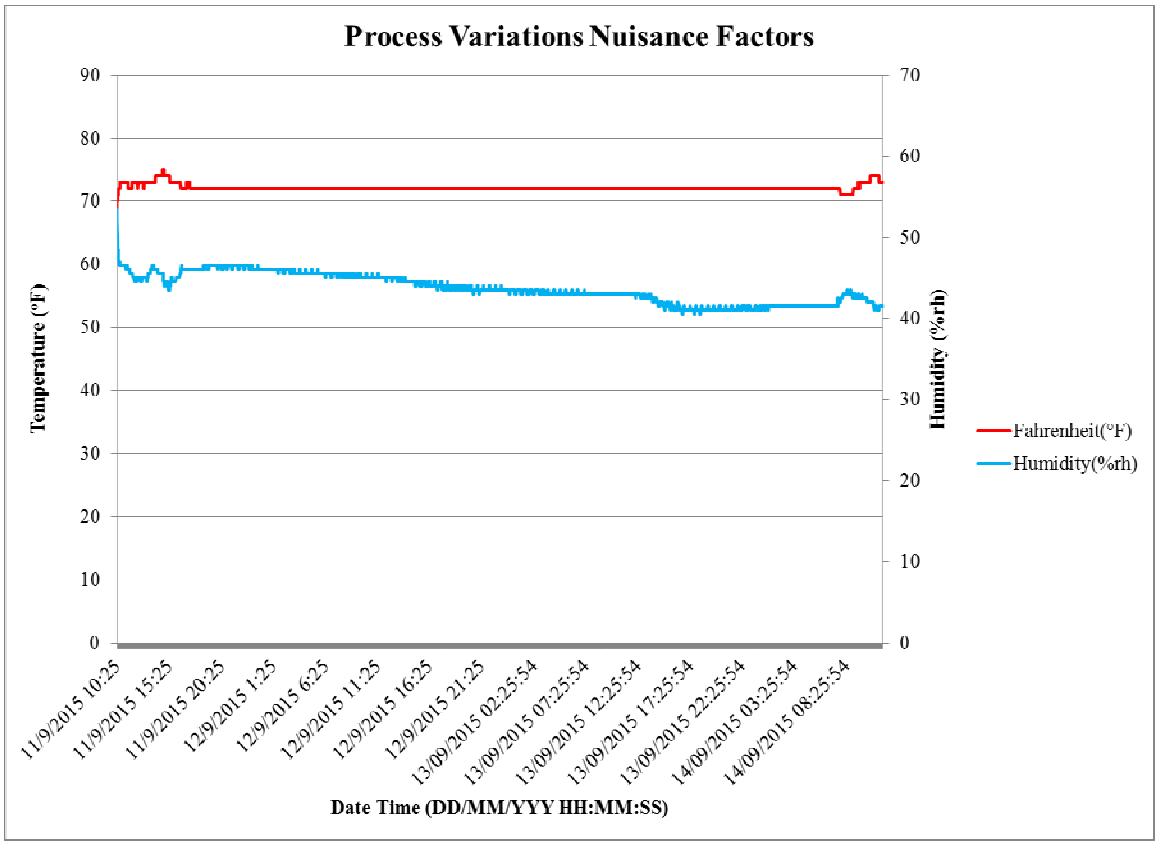


Figure 28 Process Variations Nuisance Factors

Sensitivity Analysis Test Results

The purpose of the sensitivity analysis is to reproduce a similar signal to the 305 MHz, but slightly shifted along the frequency spectrum and outside the limit of the process variations. By using five inverters instead of three the frequency shifted from 305 MHz to 225 MHz. This signal is repeated at 450 MHz with a lower magnitude as a harmonic. Board 7 was utilized in this test to validate the feasibility of detecting another

programmed signal. Figure 29 depicts the 305 MHz, 225 MHz, and the delta frequency spectrums. The 305 MHz and 225 MHz are measured in dBm0 with a range from -60 to 7 dBm0. The delta plot must be viewed in dB. The X-axis on the delta plot is from -34 to 40 dB. The delta plot shows a large peak in the middle of the spectrum (around 310 MHz) and then two small negative peaks at 225 MHz and 450 MHz. This accounts for the non-existent peaks in the 305 MHz measurement.

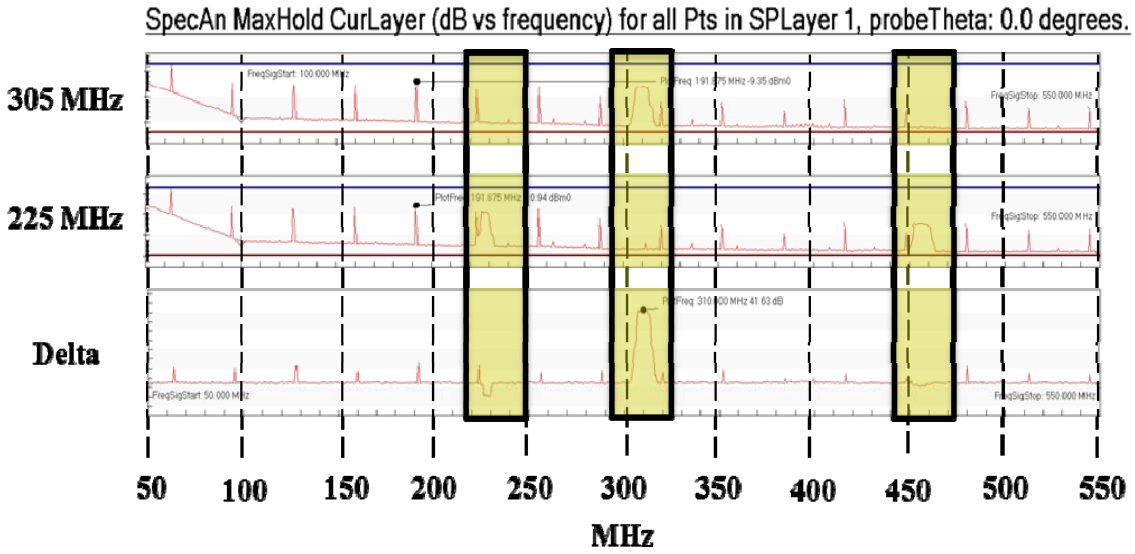


Figure 29 Sensitivity Analysis Frequency Spectrums

The frequency and magnitude plots for the sensitivity analysis are shown in Figure 30. The frequency plots have a slight color differentiation from bright green to light green demonstrating a lower dominate frequency in the upper right quadrant of the part, between the 305 MHz programmed frequency and the 225 MHz frequency. The location however, is nearly identical for the peak programmed frequencies in each test. Not only are the magnitude values for 225 MHz and 450 MHz smaller, but the widths are narrower when compared to the original 305 MHz signal.

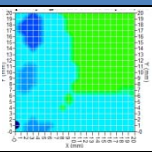
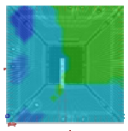
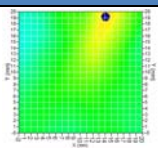
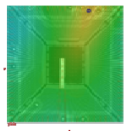
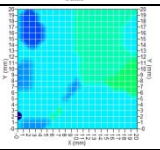
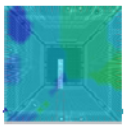
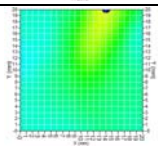
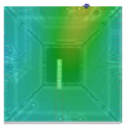
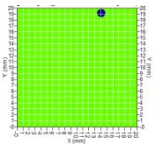
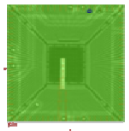
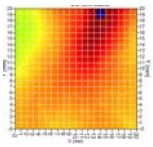
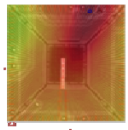
Board 7 Test	Frequency Range	Frequency (MHz)	Layered Frequency (MHz)	Mag Range	Mag (dBm0)	Layered Mag (dBm0)
305 MHz						
225 MHz						
Delta						

Figure 30 Sensitivity Analysis Frequency and Magnitude Plots by Test

Table 9 Sensitivity Analysis Table

Board 7 Test	Frequency (MHz)	Location (X, Y, Z)	Magnitude (dBm0 or dB)	Width (MHz)
305 MHz	310	(14.01, 18.98, 1.01)	-14.5	14.375
225 MHz	226.25	(13.99, 20, 1)	-18.03	9.375
450 MHz	453.125	(12.99, 20, 1)	-29.63	13.125
305 MHz Delta (Positive)	310	(14.01, 18.98, 1.01)	41.63	13.125
225 MHz Delta (Negative)	226.25	(13, 20, 1)	-33.73	6.25
450 MHz Delta (Negative)	453.125	(13, 20, 1)	-27.61	14.375

Etched Test Results

The final set of tests consisted of etching one board in a nitric and sulfuric bath for 10 seconds, using a Nisene JetEtch II. The parameters of the etch were not optimized, due to the limited number of samples to refine the process. The center of the package was etched out to expose the die and the bond wires. The purpose of this test was to examine if the package provided any signal shielding. Overall, the magnitude had a minimal

change between the package and etched part. There appears to be slightly larger area on the device that has higher magnitude.

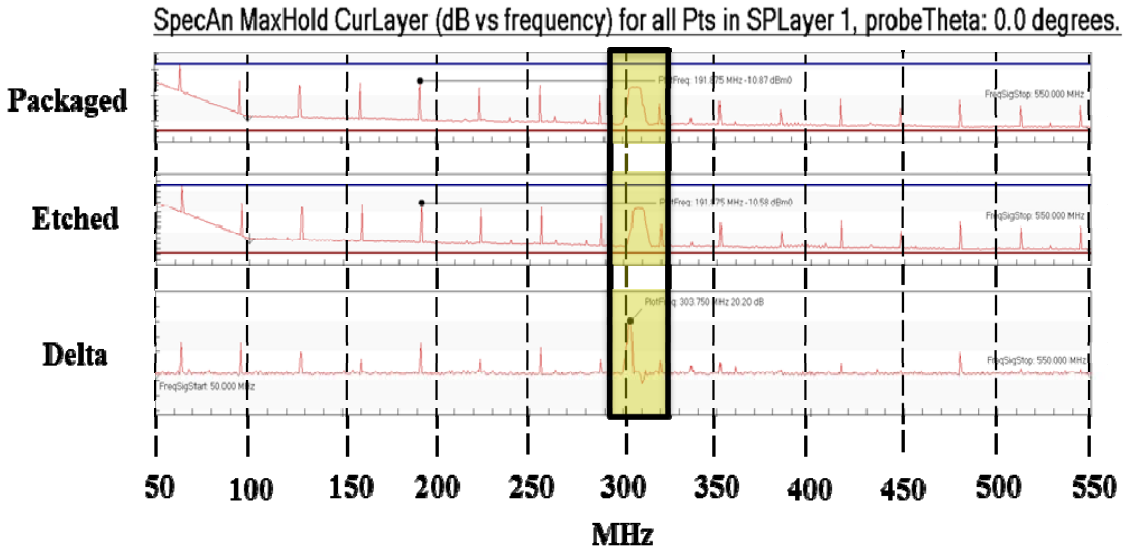


Figure 31 Etched Frequency and Magnitude Plots by Test

Board 10 Test	Freq Range	Freq (MHz)	Layered Freq (MHz)	Mag Range	Mag (dBm0)	Layered Mag (dBm0)
Packaged	650 486 421 357 292 228 164 100 MHz			7.00 -2.67 -12.14 -21.71 -31.29 -41.86 -50.43 -60.00 dBm0		
Etched						
Delta				20.00 14.43 8.86 3.29 -2.29 -7.86 -13.43 -19.00 dB		

Figure 32 Etched Frequency Spectrums

The main difference between the packaged and etched device is noticed in the width of the peak. The etched board has a narrower peak than the packaged board. This could infer that when the emission hits the package it slightly scatters the signal and creates a wider peak. Or another theory is that the dielectric properties of the package material is causing some resonances to shift slightly, and therefore increases the peak's bandwidth.

Table 10 Etched Analysis Table

Board 10 Test	Frequency (MHz)	Location (X, Y, Z)	Magnitude (dBm0 or dB)	Width (MHz)
Packaged	306.875	(12.99, 20, 1)	-16.77	14.375
Etched	307.5	(13.99, 19.99, 1)	-16.43	12.5
Delta (Positive)	303.75	(12.01, 18.98, 1.01)	20.2	5.625
Delta (Negative)	310	(12, 11, 1)	-19.53	6.875

Investigative Questions Answered

Chapter I discussed four investigative questions to be answered with this research. Each question is answered below based on the test results discussed in this chapter.

- Can counterfeit electronic parts be detected using the part's unintentional electromagnetic signature?

A part's unintentional electromagnetic signature is an indicator of a part's health, as shown in the process variation tests executed in this research. Chapter V will describe several topics of study to further this research, to provide a well-rounded answer to this question.

- How effective is the APREL EM-ISight at detecting counterfeit electronic parts?

The answer to this question is similar to the answer to the previous question. The APREL EM-ISight successfully detected and characterized a bad part during the process variation tests. The lack of peaks, at any frequency in the spectrum, is a key indicator in the identification of the defective part. This was shown in Figures 26 and 27. The system also successfully detected the programmed frequency change in the sensitivity analysis. The detection of both of the defective part in the process variation test and the programmed frequency change in the sensitivity analysis tests, provide a good foundation in the effectiveness of the APREL EM-ISight at detecting counterfeit electronic parts. In order to answer this question in its entirety more research and tests need to be conducted. Some of these suggestions are expanded upon in Chapter V.

- What is the optimal test setup to detect parts?

The DOE identified significant factors and interactions. The desirability of the two response factors were considered equally important. For this system a higher frequency magnitude and lower scan time are the desired effects of a scan. Optimizing each factor with those desired effects produced the following setting for each of the five factors: H-field probe, Z-height of 1 mm, spatial resolution of 1 mm, frequency range of 500 MHz, and a RBW of 100 Hz. These were the optimal settings for this particular device and its specific programming. This may not be the case for every device. This research has evaluated the tradeoff between resolutions, both spatially and spectrally, and time and concluded that the time saved is worth the minimal degradation in resolution.

- How repeatable are the test results?

More testing with additional parts would need to be conducted in order to answer this question with any statistical significance. The tests performed in this research infer

that scans with similar setups would provide comparable results (same peaks, relative magnitudes at those peaks, etc.), but with the limited number of samples and tests, this question cannot be answered completely. See Chapter V for recommendations on future research.

Summary

Chapter IV provided a synopsis of the results of the DOE, process variations, sensitivity analysis, and etched part tests performed in this research. This research did not exhaust all the avenues required to ensure the identification of counterfeit parts and the repeatability of test results.

V. Conclusions and Recommendations

Chapter Overview

The purpose of this research was to identify the feasibility of using APREL's EM-ISight to detect a device's inherent electromagnetic signature and use that signature to identify if a part is counterfeit or authentic. The initial steps for this research were to conduct a DOE to determine significant factors and then optimize all the factors to obtain the desired response. Several devices were measured at these optimized settings to acquire the variation in the parts, due to the manufacturer's process. A sensitivity analysis was conducted to conclude that a programmed frequency change in the same part could be detected with this measurement. Finally, an etched part was measured to show that the packaging material provided minimal shielding, but did show a change in the peak width. Chapter V provides conclusions based on the results and analysis from Chapter IV and builds on those results, to recommend future areas of research and applications.

Significance of Research

Current counterfeit detection techniques are limited in their capability to identify counterfeit electronic parts due to time, cost, and effectiveness. 3-D EM mapping with the APREL EM-ISight opens an opportunity for a non-destructive and relatively quick, cheap, and effective detection technique to recognize counterfeit electronic parts. This technique can also be utilized for other research aspects such as failure analysis, health status of a part, circuit board design layout, and parts shielding.

Recommendations for Action

Working on this research brought about two recommendations for action. The first is a camera/probe integration for image processing. A combined camera probe with image processing would increase the accuracy for pinpointing components or a specific bond wire that is emitting the signal under investigation. The current method uses an uploaded image that can be cropped and rotated to mimic the DUT. The user is then responsible for lining up the probe and that image as accurately as possible. This leaves room for human error and is not as exact as a camera integrated into the probe. The system would then perform image processing to line up the DUT for a more exact representation.

A second recommendation is the development of a small scale probe array or array of arrays that can be placed over the entire DUT for simultaneous measurement of the EME. This simultaneous measurement would be beneficial, especially for digital circuits, by taking a single snapshot instead of taking a different measurement in time, as the probe physically moves around the DUT. This was not an issue for this research, due to the simplicity of the device selected, but it will be vital for more complex devices. In addition to simultaneously taking a measurement, it would be valuable to be able to select a specific probe or subset of probes in the array for isolating a particular area.

Recommendations for Future Research

The initial recommendation for future research was originally addressed in Chapter III. The sample size is not large enough to be statistically significant. Future research should include more devices, in order to be statistically significant. In addition

to the number of devices tested, other elements can be introduced such as multiple vendors, different boards with the same device, or different versions of the same device. These different elements would add a deeper understanding of the types of variations in the EM signature that are to be expected.

Several factors can be added to the DOE to determine their impact. The main system factor that was not investigated in this research was the rotational angle of the probe. The software allows for a user to input any angle and the BDU/probe component will rotate to that angle and complete the measurement at the specified angle. This would most likely produce a different EM signature. In this research the ambient temperature and humidity were measured as a nuisance factor. Placing the DUT under multiple temperature settings, to see if it has any impact on the EM signature, would be another recommended test to better characterize a device.

Since recycled parts are one of the main contributors to counterfeit electronic parts, an ALT would help characterize a parts aging profile. This could also identify a part's remainder of usable life. An aging profile would be a key element in the detection of reused parts.

Two other recommendations include full circuit board scans and the characterization of digital boards. The addition of harmful devices, malicious code, and viruses are becoming more prevalent in counterfeit electronic parts. The identification of these features, before the part is integrated into the final platform, is crucial to retain the integrity and reliability of the system.

Conclusions of Research

This research established the viability of using APREL's EM-ISight to detect a device's inherent electromagnetic signature. A FPGA was utilized for its availability, flexibility, and ease of use. Although the classification of whether the part was a counterfeit part or not could not be determined, the system could be used as health diagnosis or failure analysis tool. Flagging a part due to its health can prompt further investigation of the integrity of the part. During the process variation tests it was obvious that Board 1 was not working properly when compared with the other 10 boards. The lack of activity and peak frequencies was a strong indicator that Board 1 was not functioning as intended.

Another finding from this research is the characterization of the tradeoff between resolution and scan time. Both spatial and spectral resolutions were assessed. The nominal improvement in the resolution did not outweigh the time saved during the scan. A 10-minute scan characterized the part just as effectively as a 4-hour scan.

Appendix A

Table 11 Assessment of counterfeit detection methods. (Guin, DiMase, & Tehranipoor, 2014)

Table 1 Assessment of counterfeit detection methods

Test Methods	Counterfeits			
	Recycled/Remarked[1]	Overproduced[2]	Out-of-spec/Defective	Cloned[2]
M1: Low Power Visual Inspection (LPVI)	D1-10, D15 -16, D19 -27, D30, D33	D1-8	D1-9	D1-8
M2: X-Ray Imaging	D17-18, D33-44	NA	D17-18, D35 -37, D41-44	D40-44
M3: Blacktop Testing	D20-26	NA	NA	NA
M4: Microblast Analysis[3]	D20-26	NA	NA	NA
M5: Package Configuration and Dimension Analysis	D11, D28	NA	D11, D28	NA
M6: Hermeticity Testing	D29, D62	D29, D62	D29, D62	D29, D62
M7: Scanning Acoustic Microscopy (SAM)	D9, D17-18, D33-44	NA	D17-18, D33 -37, D41-44	D40-44
M9: Optical Inspection	D33-40, D42 -44, D64	D35, D64	D33-40, D42 -44, D64	D40, D42-44
M10: Wire Pull	D35, D65	D35, D65	D35, D65	D35, D65
M11: Die Shear	D41	D41	D41	D41
M12: Ball Shear	D17-18	NA	D17-18	NA
M8: Scanning Electron Microscopy (SEM)	D19-27, D30 -31, D39-40, D42-44	NA	D42-44	D40, D42-44
M13: X-Ray Fluorescence (XRF)	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M14: Fourier Transform Infrared Spectroscopy (FTIR)	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M15: Ion Chromatography (IO)	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M16: Raman Spectroscopy	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M17: Energy Dispersive X-Ray Spectroscopy (EDS)	D12-14, D30 -32, D57-59	D57-59	D30-32, D57-59	D57-59
M18: Parametric Tests	D33-36, D38 -40, D42, D45 -50, D56	D45-50	D33-36, D38 -40, D42, D45 - 50, D56	D40, D42, D45-50, D56
M19: Functional Tests	D33-36, D38 -40, D42, D51 -56, D61, D63 -65	D51-56,D61, D63-65	D33-36, D38 -40, D42, D51 -56, D61, D63 -65	D42, D51 -56, D61, D63-65
M20: Burn-In Tests	D34-42, D50 -51, D53-54, D56, D61, D63-65	D50-51, D53-54, D56, D61, D63-65	D34-42, D50 -51, D53-54, D56, D61, D63-65	D40-42, D50 -51, D53-54,D56, D61, D63-65
M21: Structural Tests	D34-42, D47, D51-56	D47, D51-56	D34-42, D47, D51-56	D40-42, D47, D51-56

[1]The recycled and remarked parts are highly correlated. Remarking is a part of recycling. Thus, remarked parts can be recycled. Also, remarking for new parts to change the specifications involves recycling

[2]We can only detect overproduced, and cloned counterfeit types if there are counterfeit defects present in them

[3]After microblasting, the materials are collected and send to material analysis

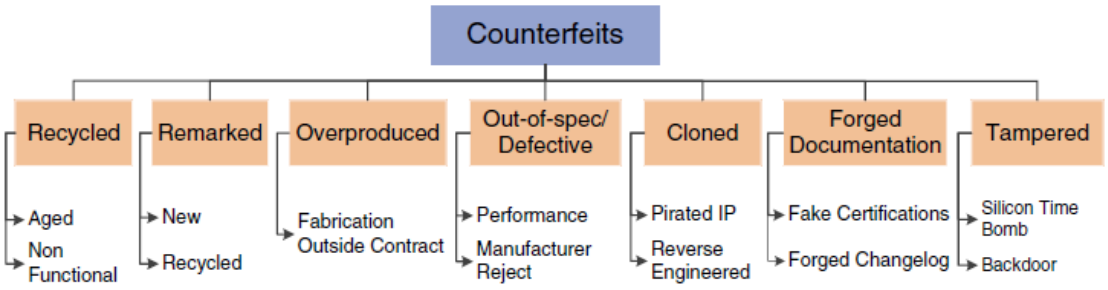


Figure 33 Taxonomy of counterfeit component types. (Guin, DiMase, & Tehranipoor, 2014)

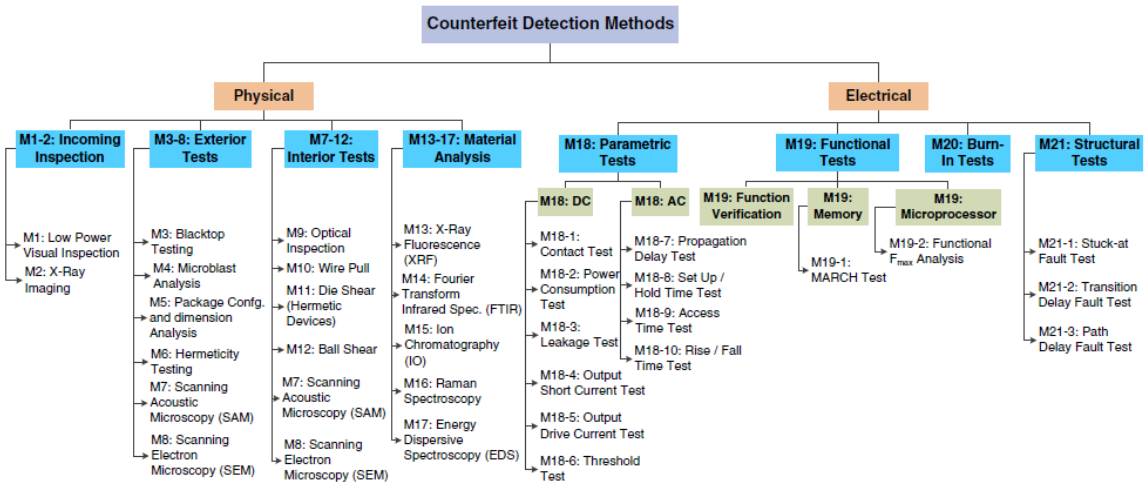


Figure 34 Taxonomy of counterfeit detection methods. (Guin, DiMase, & Tehranipoor, 2014)

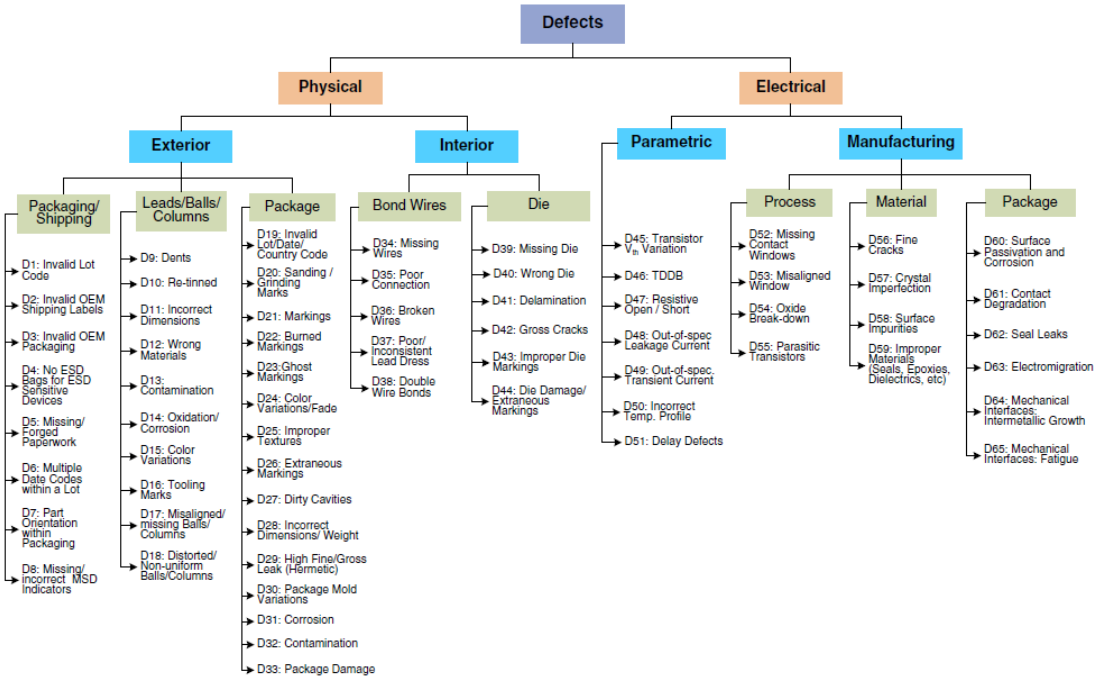


Figure 35 Taxonomy of defects and anomalies present in counterfeit electronic components. (Guin, DiMase, & Tehranipoor, 2014)

Appendix B

Setup Data

Probe

Name: APRL_701-00113_H-Probe_6GHz_Broad6GhzLNA w/Shield
Serial Number: 701-00113
Probe Type: H_xy
Frequency Range: 10 KHz to 6 GHz
Model: ALS-EMIS-P-H-M2.2
Compensation Value: 0
Calibration Date: 3/24/3015
Calibration Standard: IEC 61967-6 2002
Ch_dB_APRL: 27.5041099464328
Ch_dB_IEC: 0

Probe Factor Table

Freq (MHz)	Hx_dB Target (dB A/m)	Vp_m (dBm)	Vp_r (dBV)	Cf_dB (dB S/m)	K1_dB	K2_dB	K3_dB
0.0100	-18.20	-123.70	-136.71	121.11	-2.60	0.00	0.00
0.1000	-18.20	-111.50	-124.51	108.91	-2.60	0.00	0.00
100.0000	-18.20	-56.40	-69.41	53.81	-2.60	0.00	0.00
300.0000	-18.20	-47.90	-60.91	45.31	-2.60	0.00	0.00
835.0000	-18.20	-39.20	-52.21	36.61	-2.60	0.00	0.00
900.0000	-18.20	-37.70	-50.71	35.11	-2.60	0.00	0.00
1600.0000	-18.20	-37.20	-50.21	34.61	-2.60	0.00	0.00
1800.0000	-18.20	-37.10	-50.11	34.51	-2.60	0.00	0.00
1900.0000	-18.20	-36.30	-49.31	33.71	-2.60	0.00	0.00
2450.0000	-18.20	-33.70	-46.71	31.11	-2.60	0.00	0.00
3500.0000	-18.20	-36.80	-49.81	34.21	-2.60	0.00	0.00
5200.0000	-18.20	-37.00	-50.01	34.41	-2.60	0.00	0.00
5800.0000	-18.20	-34.50	-47.51	31.91	-2.60	0.00	0.00
6000.0000	-18.20	-39.70	-52.71	37.11	-2.60	0.00	0.00

Probe

Name: APRL_710-00106_E-Probe_6GHz_Broad6GhzLNA
Serial Number: 710-00106
Probe Type: H_xy
Frequency Range: 10 KHz to 6 GHz
Model: ALS-EMIS-P-E-M2.2
Compensation Value: 0
Calibration Date: N/A
Calibration Standard: IEC 61967-6 2002
Ch_dB_APRL: 27.5041099464328
Ch_dB_IEC: 0

Probe Factor Table

Freq (MHz)	Hx_dB Target (dB A/m)	Vp_m (dBm)	Vp_r (dBV)	Cf_dB (dB S/m)	K1_dB	K2_dB	K3_dB
0.0100	29.34	-143.50	-156.51	140.91	44.94	0.00	0.00
0.1000	29.34	-123.50	-136.51	120.91	44.94	0.00	0.00
100.0000	29.34	-68.50	-81.51	65.91	44.94	0.00	0.00
300.0000	29.34	-54.50	-67.51	51.91	44.94	0.00	0.00
835.0000	29.34	-47.10	-60.11	44.51	44.94	0.00	0.00
900.0000	29.34	-45.70	-58.71	43.11	44.94	0.00	0.00
1600.0000	29.34	-44.10	-57.11	41.51	44.94	0.00	0.00
1800.0000	29.34	-44.10	-57.11	41.51	44.94	0.00	0.00
1900.0000	29.34	-44.20	-57.21	41.61	44.94	0.00	0.00
2450.0000	29.34	-41.80	-54.81	39.21	44.94	0.00	0.00
3500.0000	29.34	-43.70	-56.71	41.11	44.94	0.00	0.00
5200.0000	29.34	-48.60	-61.61	46.01	44.94	0.00	0.00
5800.0000	29.34	-46.10	-59.11	43.51	44.94	0.00	0.00

Signal Path Table

Freq (MHz)	PreAmp (dB)	BDU loss (dB)	C1 loss (dB)	C2 loss (dB)	C3 loss (dB)
0.0100	15.90	0.00	-0.10	-0.10	-0.20
0.1000	17.60	0.00	-0.10	-0.10	-0.20
100.0000	32.00	0.00	-0.40	-0.30	-0.40
300.0000	31.90	0.00	-0.60	-0.50	-0.70
835.0000	32.10	0.00	-0.90	-0.90	-1.20
900.0000	32.10	0.00	-1.00	-1.00	-1.30
1600.0000	32.60	0.00	-1.30	-1.30	-1.70
1800.0000	32.50	0.00	-1.30	-1.30	-1.80
1900.0000	32.50	0.00	-1.40	-1.40	-1.80
2450.0000	32.80	0.00	-1.60	-1.50	-2.10
3500.0000	32.40	0.00	-1.90	-1.80	-2.50
5200.0000	32.30	0.00	-2.30	-2.20	-3.10
5800.0000	31.80	0.00	-2.40	-2.40	-3.30
6000.0000	32.00	0.00	-2.50	-2.40	-3.30

Pre-Amp

Name: BroadBand_6GHz
Input Impedance: 50 ohm
Frequency Span: 0.010 to 6 GHz
Linearity: +/- 1.5 dB
Dynamic Range: 13 dBm
Calibration Date: 3/24/3015

Micro-Stripline

Name: APREL_MSL_6GHz
Serial No: 690-00109
Vs (dB V): -13.01 db V
h (mm): 0.6 mm

w (mm): 1 mm
Impedance (dB): 50 ohm
Calibration Date: 3/24/3015

BDU

Name: default_LineLoss 4.1
Description: Sum of BDU_L C1_L C2_L C3_L
Serial No: Do not modify this record
Model: 0001
Calibration Date: N/A

Cable 1 loss

Name: default_C1Loss
Description:
Serial No: SN 642-00113
Model:
Calibration Date: 3/24/3015

Cable 2 loss

Name: default_C2Loss
Description:
Serial No: SN 642-00112
Model:
Calibration Date: 3/24/3015

Cable 3 loss

Name: default_C3Loss
Description:
Serial No: SN 642-00114
Model:
Calibration Date: 3/24/3015

Instrument

SA Settings Name: 300 MHz
SA Serial No: B010217
Model: TEKTRONIX-RSA6120A
Calibration Date: 11/8/2015
Start Frequency: 50
Stop Frequency: 550
Frequency Step: 0.624219725343321
Frequency Units: MHz
AutoRBW: False
Resolution Bandwidth (RBW): 100 Hz
AutoVBW: True
Video Bandwidth (VBW): 5 Hz

AutoAtt: True
Attenuation (dB): 25
Sweep Time (us): 0 us
Sweep Count: 1
Reference Level (dB): 0
EMITraceSize : 801
TraceSize : 801
TraceCompression : 0
ViewMode : RTSA_Mode
DetectionMode : PK+
FunctionMode : Normal
DPXFreqStep : 0
DPXDwellTime : 0
DPXDotPersistance : 0

Using probe calibration: StartF:50 StopF:550 probe Cf freq: 300 Cf_dB = 45.31.

Device Under Test (DUT)

Name: FPGA
Serial No.: 1
Width: 20 mm
Height: 20 mm
Reference Point Denso WT(X,Y,Z): 135.28 , 153.24 , 23.66
DUT Description: Lg Board

Measurement Profile

Profile Name: FPGA_Test

Number of layers: 1

Bibliography

Aerospace Industries Association. "A Special Report Counterfeit Parts: Increasing Awareness and Developing Countermeasures." March 2011. *http://www.aia-aerospace.org/assets/counterfeit-web11.pdf.* PDF. 5 3 2015.

APREL. *http://www.aprel.com/#!about/c1714*. n.d. 11 3 2015.

Boyer, Alexandre, et al. "Characterization of the Evolution of IC Emissions After Accelerated Aging." *Electromagnetic Compatibility, IEEE Transactions (Volume:51 , Issue: 4)* (2009): 892-900.

Boyer, Alexandre, et al. "Experimental Investigations into the Effects of Electrical Stress on Electromagnetic Emission from Integrated Circuits." *Electromagnetic Compatibility, IEEE Transactions (Volume:56 , Issue: 1)* (2013): 44-50.

Cicchiani, John A., et al. "Analysis of electromagnetic emissions to determine UUT health ." *AUTOTESTCON, 2008 IEEE* (2008): 557-561.

Cobb, William E, et al. "Intrinsic Physical-Layer Authentication of Integrated Circuits." *Information Forensics and Security, IEEE Transactions* (2011): 14-24.

Cobb, William E., et al. "Physical Layer Identification of Embedded Devices Using RF-DNA Fingerprinting." *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010* (2010): 2168-2173.

Cohen, Jacob. "A Power Primer." *Psychological Bulletin* (1992): 155-159. PDF.

Contreras, Gustavo K., Tauhidur Rahman and Mohammad Tehranipoor. "Secure Split-Test for Preventing IC Piracy by Untrusted Foundry and Assembly." *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2013 IEEE International Symposium* (2013): 196-203.

CTI. "Counterfeit Components Avoidance Programe, Certification For." 11 7 2013. *http://www.cti-us.com/pdf/CCAP101Certification.pdf.* PDF. 8 5 2015.

DARPA IRIS. *http://www.darpa.mil/Our_Work/MTO/Programs/Integrity_and_Reliability_of_Integrated_Circuits_(IRIS).aspx*. n.d. 11 3 2015.

DARPA SHIELD.
http://www.darpa.mil/Our_Work/MTO/Programs/Supply_Chain_Hardware_Integrity_for_Electronics_Defense_(SHIELD).aspx. n.d. 11 3 2015.

DARPA TRUST.
http://www.darpa.mil/Our_Work/MTO/Programs/Trusted_Integrated_Circuits_(TRUST).aspx. n.d. 11 3 2015.

Delta.
"http://www.madebydelta.com/imported/images/DELTA_Web/documents/ME/Product%20Info/1131%20SAM(2).pdf." n.d. *Scanning Acoustic Microscopy (SAM).* PDF. 23 3 2015.

DiBene II, Joseph T. and James L. Knighten. "Effects of device variations on the EMI potential of high speed digital integrated circuits." *Electromagnetic Compatibility, 1997. IEEE 1997 International Symposium* (1997): 208-212.

Frederico, Joseph. "Detecting Counterfeit Electronic Components." n.d.
http://www.erai.com/CustomUploads/ca/wp/2009_3Detecting_Counterfeit_Electronic_Components.pdf. PDF. 02 March 2015.

Gadget Factory. *http://store.gadgetfactory.net/papilio-pro/*. 2015. 25 6 2015.

Government-Industry Data Exchange Program. *http://www.gidep.org/gidep.htm*. n.d. 10 3 2015.

Guin, Ujjwal, Daniel DiMase and Mohammad Tehranipoor. "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead." *Springer Science+Business Media New York* (2014).

Guin, Ujjwal, Daniel DiMasse and Mohammad Tehranipoor. "A Comprehensive Framework for Dounterfeit Defect Coverage Analysis and Detection Assessment." 15 1 2014.
http://www.engr.uconn.edu/~tehrani/publications/jetta14.pdf. PDF. 8 5 2015.

In Compliance. *http://incompliancemag.com/article/novel-approaches-for-the-detection-of-counterfeit-electronic-components/*. 1 Oct 2010. 12 3 2015.

International Chamber of Commerce. *Estimating the global econmoic and social impacts of counterfeiting and piracy*. London: Frontier Economics Ltd, 2011.

Kessler, Lawrence W. and Thomas Sharpe. "Faked Parts Detection." 03 June 2010. *http://smtcorp.com/ext/manual/united-el-article-2012-08-22.html.* 02 March 2015.

Koushanfar, Farinaz and Gang Qu. "Hardware Metering." *Design Automation Conference, 2001. Proceedings* (2001): 490-493.

Lowry, Robert K. "Ors Labs." 2007. *http://www.ors-labs.com/pdf/MASH07CounterfeitDevice.pdf.* PDF. 5 3 2015.

McCants, Carl. *http://www.iarpa.gov/index.php/research-programs/tic*. n.d. 8 5 2015.

Montanari, I, A. Tacchini and M. Maini. "Impact of thermal stress on the characteristics of conducted emissions." *Electromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium* (2008): 1-4.

Montanari, Ivan. "EMI measurements for aging control and fault diagnosis in active devices." *Electromagnetic Compatibility and Electromagnetic Ecology, 2005. IEEE 6th International Symposium* (2005): 183-186.

Muccioli, James P., Terry M. North and Kevin P. Slattery. "Characterization of the RF emissions from a family of microprocessors using a 1 GHz TEM cell." *Electromagnetic Compatibility, 1997. IEEE 1997 International Symposium* (1997): 203-207.

National Defense Industrial Association. *http://www.ndia.org/Resources/Documents/TopIssues_2014.pdf*. 2014. PDF. 23 3 2015.

Pathak, Bogdan A. and Walter J. Keller. "Advanced Detection of Electronic Counterfeits." 19 April 2013. *http://www.nokomisinc.com/.* PDF of PowerPoint Presentation. 2015.

Rostami, Masoud, Farinaz Koushanfar and Ramesh Karri. "A Primer on Hardware Security Models Methods and Metrics." *Proceedings of the IEEE* (2014): 1238-1295.

Sawyer, Don. *http://mil-embedded.com/articles/counterfeit-taking-malicious-turn/*. 6 10 2014. 8 5 2015.

Services, U.S. Senate Committee on Armed. "Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms." 2 2012. *http://www.gao.gov/assets/590/588736.pdf.* 8 5 2015.

U.S. Department of Commerce. "Defense Industrial Base Assessment: Counterfeit Electronics." Jan 2010. *http://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010.* PDF. 02 March 2015.

US Congress. "National Defense Authorization Act for Fiscal Year 2012." n.d. *http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf.* PDF. 8 5 2015.

Wang, Xiaoxiao and Mohammad Tehranipoor. "Novel Physical Unclonable Function with Process and Environmental Variations." *IEEE* (2010): 1065-1070. PDF.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
24-12-2015	Master's Thesis	January 2015 – November 2015

TITLE AND SUBTITLE

Investigation of Electromagnetic Signatures of a FPGA Using an APREL EM-ISIGHT System

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Sutherlin, Karynn A., BSEP, Civilian, DAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENV-MS-15-D-035

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
<intentionally left blank>

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRUBTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT
Large military platforms have encountered major performance and reliability issues due to an increased number of incidents with counterfeit electronic parts. This has drawn the attention of Department of Defense (DOD) leadership making detection and avoidance of counterfeit electronic parts a top issue for national defense. More defined regulations and processes for identifying, reporting, and disposing of counterfeit electronic parts are being revised to raise awareness for this aggregating issue, as well as enhance the detection of these parts. Multiple technologies are currently employed throughout the supply chain to detect counterfeit electronic parts. These methods are often costly, time-consuming, and destructive. This research investigates a non-destructive test method that collects unintentionally radiated electromagnetic emissions from functional devices using a commercially available system, the APREL EM-ISight. A design of experiments (DOE) is created and exploited to determine the optimal test settings for measuring devices. The sensitivity of the system is analyzed by scanning a commercial-off-the-shelf (COTS) field-programmable gate array (FPGA) at the optimal test settings established from the DOE and varying the programmed signal. This research established the viability of using APREL's EM-ISight to detect a device's inherent electromagnetic signature. Another take away from this research is the tradeoff between resolution and scan time.

15. SUBJECT TERMS
Electromagnetic, counterfeit, FPGA,

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Lt Col Kyle Oyama, AFIT/ENV
U	U	U	UU	88	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4352 (kyle.oyama@afit.edu)